The Dark Side of E-Commerce: Dropshipping Abuse as a Business Model

Arjun Arunasalam[†*], Andrew Chu[‡*], Muslum Ozgur Ozmen[†], Habiba Farrukh[¶], and Z. Berkay Celik[†]
[†] Purdue University, {aarunasa, mozmen, zcelik}@purdue.edu
[‡] University of Chicago, andrewcchu@uchicago.edu
[¶] University of California, Irvine, hfarrukh@uci.edu

***Abstract*—The impact of e-commerce on today's society is a global phenomenon. Given the increased demand for online purchases of items, e-commerce platforms often defer item sales to third-party sellers. A number of these sellers are *dropshippers*, sellers acting as middlemen who fulfill their customers' orders through third-party suppliers. While this allows customers to access more products on e-commerce sites, we uncover that abusive dropshippers, who exploit the standard permitted dropshipping model, exist, deceiving customers, and damaging other e-commerce sellers. In this paper, we present the first comprehensive study on the characterization of abusive dropshippers and uncover harmful strategies they use to list items and evade account suspension on e-commerce marketplaces. We crawled the web to discover online forums, instructional material, and software used by the abusive dropshipping community. We inductively code forum threads and instructional material and read software documentation, installing when possible, to create an end-to-end lifecycle of this abuse. We also identify exploitative strategies abusive dropshippers use to ensure persistence on platforms. We then interviewed six individuals experienced in e-commerce (legal consultants and sellers) and developed an understanding of how abusive dropshipping harms customers and sellers. Through this, we present five characteristics that warrant future investigation into automated detection of abusive dropshippers on e-commerce platforms. Our efforts present a comprehensive view of how abusive dropshippers operate and how sellers and consumers interact with them, providing a framework to motivate future investigations into countering these harmful operations.**

I. Introduction

The convenience of purchasing products over the internet has caused a 55% rise in online spending and more than half a trillion more transactions compared to pre-pandemic levels [28], [32], [33]. In response, e-commerce platforms such as Amazon, Shopify, Wish, and eBay offer greater accessibility and variety of products to their customers globally. As a result, existing "marketplace" environments have grown, with an increase in independent sellers who list items and fulfill customer orders.

A popular fulfillment method of independent sellers is *dropshipping* [31], [67], a form of retail business in which e-sellers establish *formal selling agreements* with third-party suppliers or source vendors, to fulfill customers' orders without holding physical item stock. An e-commerce seller implementing a dropshipping business is called a *dropshipper*. These formal agreements allow dropshippers to (1) leverage source vendors' fulfillment supply chain and (2) brand the items supplied by the third-party seller as their own, in exchange for a fee or percentage of sale profit. For instance, a dropshipper who wishes to sell pet toys first reaches out to a source vendor who manufactures pet toys and establishes a formal selling agreement. After confirming the agreement, the dropshipper lists the products of the partnered supplier as their own in an e-commerce marketplace store. On receiving a customer order, the dropshipper forwards the order information to their partnered supplier. Their supplier then ships the purchased item(s) to the customer on behalf of the dropshipper, and the dropshipper makes sales without holding physical item stock.

Dropshipping is governed by e-commerce platform regulations, defining the responsibilities of dropshippers on item fulfillment, handling returns or damaged products, and paying sales tax [4], [6], [36], [87]. Despite regulations, we have seen a recent proliferation of exploitative sellers who abuse this business model for economic gain in "get-rich-quick schemes" [16], [45], [98]. These sellers, whom we refer to as *abusive dropshippers*, circumvent regulations to profit from the efforts of other sellers while exerting minimum effort in running an *abusive dropshipping* business.

Similar to conventional dropshippers, abusive dropshippers do not keep physical stock of their products. However, they do not establish formal selling agreements with source vendors and instead directly list items of other e-commerce sellers on their own marketplace stores. On receiving a customer order, an abusive dropshipper purchases the ordered item using the customer's name and shipping address from another e-commerce seller who ships the order to the customer. In this way, abusive dropshippers execute an exploitative method of item sourcing to fulfill customer orders without notifying sellers of the items they sell. For instance, abusive dropshippers may source items from Amazon and sell them on their own website for three times the price the original seller lists them for [90]. Customers are unaware that they purchase from an abusive dropshipper, and original sellers are unaware they fulfill an abusive dropshipper's order.

Abusive dropshippers profit from listing products that are not theirs, harming e-commerce stakeholders. They disservice customers by not personally fulfilling orders (e.g., neglected orders due to lack of stock, missing tracking numbers) and exploit other sellers by listing their items without permission.

[*]Authors Arunasalam and Chu made equal contributions to this work.

Network and Distributed System Security (NDSS) Symposium 2024
26 February - 1 March 2024, San Diego, CA, USA
ISBN 1-891562-93-2
https://dx.doi.org/10.14722/ndss.2024.23039
www.ndss-symposium.org

Abusive dropshipping is attractive to prospective malicious e-commerce sellers because it can be quickly configured, is highly profitable, and requires minimal maintenance. To detail, the lack of formal agreements with source vendors allows an abusive dropshipper to immediately accept customer orders and payment after listing an item in their store. Here, they avoid time spent negotiating a formal selling agreement and maintaining this partnership. The lack of partnership also allows an abusive dropshipper to list nearly any item they wish, easily catering to many e-commerce customers.

Abusive dropshippers additionally have the flexibility of selling items without requiring physical presence in the country where they list their products. They exploit this flexibility by listing items in one country and fulfilling them from another country by leveraging e-commerce platforms that offer international shipping. For instance, an abusive dropshipper in Turkey observes a popular personal care product (e.g., cosmetic, men's grooming products) is available from another e-commerce seller in the United States, but not listed on any marketplace in Mexico[1]. Since there is no competition, the abusive dropshipper lists these products for much higher prices than the combined cost of purchasing this item from another e-commerce seller and paying shipping costs to customers in Mexico.

This ease of execution and generation of profit has led to a thriving global underground community where individuals discuss a variety of abusive dropshipping-related topics, e.g., finding profitable and regional popular products, software to know the availability of popular online product sales in a specific country, and fake order tracking services.

Despite the malicious effects brought on by abusive dropshippers, it is difficult for e-commerce platforms to effectively implement abusive dropshipping prevention measures [7], [9], [35], [88], as abusive dropshippers' non-conventional methods of operation are challenging to identify. Current customer protection methods employed by e-commerce platforms rely mostly on manual reporting of offending sellers [8], [37], [89]. Platforms suspend or remove a seller from their marketplace only when a certain volume of reports is reached for that seller. This allows abusive dropshippers to persist in marketplaces, continuing to deceive customers and other sellers.

Previous technical community efforts have explored e-commerce fraud focusing on buyer-initiated abusive behavior, e.g., credit card fraud [77], and suspicious shopping patterns [113]. Other works examining the reshipping mule monetization scheme [49] and concession abuse scam [92] (both also buyer-initiated) come closest to exploring similar fraudulent operations on e-commerce platforms. However, these works differ in regard to operation and parties involved. As such, we see that work examining seller-initiated e-commerce fraud, specifically dropshipping, is largely absent.

In this paper, we present the first study characterizing abusive dropshippers and uncover how their strategies harm customers, other sellers, and e-commerce platforms. To accomplish this, we collected abusive dropshipping-related keywords, which we developed by analyzing dropshipping-related materials from an initial crawl. We discovered seven forums where abusive dropshipping discussion occurs. We crawled these forums and collected $3{,}651$ relevant discussion threads.

[1]Countries align with discussions from our studied forums.

To understand how abusive dropshippers operate their stores and uncover strategies they use to evade account suspension for exploitative monetization, we randomly sampled threads and conducted inductive coding until we reached thematic saturation at $1{,}050$ threads. We discovered references to instructional material and software tools. We analyzed four instructional materials by inductively coding text guides and transcripts of 86 video guides. We then studied the execution behavior of 13 most frequently mentioned software tools to understand how software amplifies abusive dropshipping. We also sought to understand how the operation can impact sellers, customers, and e-commerce platforms. To accomplish this, we interviewed six individuals with e-commerce expertise who were either (1) legal consultants to sellers affected by abusive dropshipping or (2) experienced sellers on e-commerce platforms.

Our analysis reveals exploitative strategies consistent across forums, instructional material, and interviews. These strategies lead to abusive consequences harming e-commerce stakeholders: customers, sellers, and the platform. To illustrate, because abusive dropshippers have no access to information about their private seller's inventory, customers may never receive orders when the private seller has no stock or have tracking numbers withheld/provided fake numbers. These experiences harm sellers whose products' reputation is affected by online reviews/posts from customers with negative experiences. Abusive dropshippers' consequences can propagate harm to the platform, due to the negative experiences of customers and sellers that, in turn, impact platform traffic.

With the knowledge of abusive dropshipping operation modes and software use, we discovered five distinct traits associated with abusive dropshippers, such as listing items with a high distinct brand count and low pricing range. Our findings motivate further investigation into how abusive dropshippers on e-commerce platforms operate and methods to mitigate the harm caused by abusive dropshippers to users.

In this work, we make the following contributions:

- We present the first study of abusive dropshipping on e-commerce platforms by discovering and examining discussion forums and software used in this community.
- We conducted semi-structured interviews with legal consultants and sellers to understand how abusive dropshipping can impact e-commerce parties.
- We identify and characterize abusive dropshipping techniques that harm customers, other sellers on e-commerce platforms, and the platforms themselves.
- We present five distinct abusive dropshipping characteristics that can inform users of this activity online.

Ethical Considerations & Responsible Disclosure. The data we analyze in this work comprise online communications, software, and interview data. For online communication data, we take the following steps to preserve privacy and minimize re-identification risks. Our data collection recorded only non-sensitive information. We collected and analyzed forum threads, and did not examine usernames, locations, or any account metrics that may reveal a user's identity. For forum posts quoted in this paper, we provide only relevant fragments/paraphrases from original quotes. For software, we analyze tools found by studying forums, which are publicly accessible. To avoid supporting exploitative material, we did not pay for tools/guides

marketed for such purposes and only examined available public content, such as descriptions, free video previews, and tutorials on YouTube channels. For interview data, we did not collect any personally identifiable information and anonymized participant identities. Our study was considered exempt by our IRB.

As our findings present a selling method that harms e-commerce platforms, customers, and other sellers, we prepared a report detailing abusive dropshippers' abusive strategies and harm. We shared the report with 10 e-commerce platforms[2] and the Federal Trade Commission (FTC) via relevant channels. Our reports are being reviewed by these parties and we are currently coordinating with them for next steps.

II. Background and Motivation

A. Dropshipping E-commerce

Dropshipping is a form of retail business where the seller establishes formal agreements (i.e., supply contracts) with source vendors to handle customers' orders without holding physical item stock [31], [67]. Dropshippers can host their business on various e-commerce platforms, such as Shopify, eBay, Etsy, and Amazon, where each platform presents different advantages and disadvantages. For example, Shopify offers low transaction fees but has comparatively lower consumer traffic than established big-box e-commerce sites (e.g., Amazon). Dropshippers can also sell a variety of items on these platforms, selecting them by various means, such as through market research, personal interest, and current item availability.

Dropshipping is regulated under regulations defined by e-commerce platforms. We refer to dropshippers who follow platform regulations as *compliant dropshippers*, conducting dropshipping operations that accommodate e-commerce guidelines. We studied the regulations of four major e-commerce platforms (eBay [36], Amazon [6], Shopify [87], AliExpress [4]) to understand the compliant dropshipping process. Fig. 1-ⓐ illustrates the three phases of a compliant dropshipper operation, involving themselves, source vendors, and customers.

Sourcing Items. Before listing items to sell, a compliant dropshipper must establish a formal agreement with the source vendor(s) that carries their items (❶). For instance, a USA dropshipper enters an agreement with a Japanese premium kitchenware supplier. The supplier agrees to a price of $80 per chef's knife, which the dropshipper lists for $120.

The agreement consists of two parts: (a) the vendor agrees to fulfill the customer orders of the compliant dropshipper, and (b) the compliant dropshipper agrees to be listed as the source shipping address on the package. With part (a), the compliant dropshipper is guaranteed an allotted quantity of the vendor's item stock, for any item(s) detailed in the formal agreement. This ensures all customer orders for the dropshipper will be fulfilled in a consistent and timely manner. Part (b) transfers all legal liability for customer interactions (including returns/refunds and customer support) from the source vendor to the compliant dropshipper. Dropshippers may source items via bulk sourcing (all listings from a single source vendor) and independent sourcing (items from multiple source vendors) [30].

Item Fulfillment. A compliant dropshipper opens their store on an e-commerce platform after establishing agreement with source vendor(s), allowing consumers to begin purchasing their items (❷). On receiving customer orders, compliant dropshippers fulfill purchases in one of two ways: (a) source vendor fulfillment and (b) fulfillment services (❸).

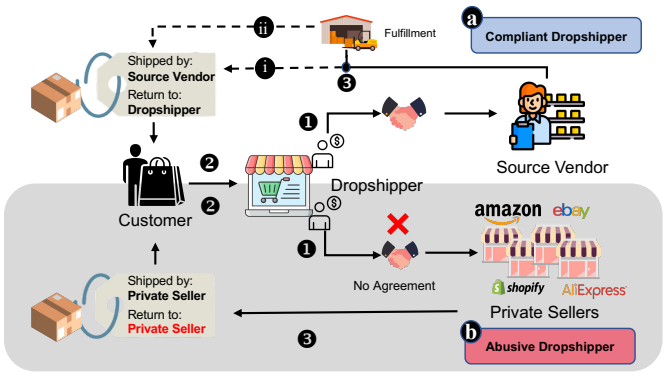

Fig. 1: Compliant and abusive dropshippers' operations.

In source vendor fulfillment, a dropshipper forwards customers' information to the source vendor(s), who then fulfills the order, dispatching customers' items using shipping labels containing the dropshipper's contact information (ⓘ). In fulfillment services, the dropshipper pays a fee for a third-party service that physically stores items and ships them to customers (e.g., Amazon's Fulfilled by Amazon (FBA) service [5] and Rakuten Logistics [79]). Here, a dropshipper will instruct the source vendors to ship customers' orders to the fulfillment service's warehouse, from where they will then be forwarded to the customer (ⓘⓘ). These services simplify item returns or refunds by multiplexing items from potentially many source vendors to one location that the dropshipper can later manage.

B. Abusive Dropshipping

An abusive dropshipper models their operation after compliant dropshipping but covertly sources items in their exploit (Fig. 1-ⓑ). To start the abusive dropshipping operation, they first decide on two e-commerce platform domains: (1) the *source* domain, from which they fulfill customers' items via other sellers, and (2) the *target* domain, where they list items for customers to buy. After deciding on *source* and *target* domains, abusive dropshippers proceed to sourcing items to sell.

Abusive Items Sourcing. Abusive dropshippers do *not* establish formal agreements with source vendors of the items they list on their *target* domain (❶). Thus, they violate e-commerce platform regulations by listing a private seller's items without said seller's consent or knowledge. In this work, we refer to sellers exploited by abusive dropshippers as *private sellers*.

Exploitative Fulfillment. The abusive dropshipper chooses a single or multiple *target* domain(s) in a country to market goods to customers. Common *target* domains include e-commerce platforms such as Amazon, Flipkart, or AliBaba. Some abusive dropshippers host their own commerce websites as *target* domains via services such as Shopify. To fulfill a customer's order (placed on a *target* domain-❷), the abusive dropshipper buys the desired item(s) from a private seller using the customer's shipping information. The private seller uses their own label and address to ship the order placed by the abusive

[2]Amazon, eBay, Flipkart, Etsy, Wish, Noon, Shopify, Myantra, Wal-Mart, and Coppel

dropshipper (❸). Customers are unaware that other private sellers fulfill their orders, and private sellers are unaware that the customer is not the one directly placing the order.

To understand if these operations abide by platform guidelines for selling, we analyze the guidelines for 20 e-commerce platforms. We selected popular platforms serving diverse regions - Asia, Africa, North America, South America, and Europe. Our analysis shows that abusive dropshippers' operations clearly violate e-commerce guidelines of appropriate selling conduct. Because abusive dropshippers do not have an agreement/contract with their "supplier" (private seller), their operations violate platform rules for (1) agreement/communications with suppliers, (2) shipping and packaging requirements, and (3) control of stock requirements (e.g., ensuring sufficient stock for an existing listing). We present a summary of relevant excerpts from platform guidelines in Appendix Table V.

Because these operations violate guidelines stipulated by the e-commerce platform, we refer to such operations as *abusive* dropshipping. This framing is consistent with works violating online platforms' guidelines, such as toxic content [95], misinformation [64] and search-rank manipulation [78], which the S&P community has long explored.

Example Abusive Dropshipping Operation. We illustrate an operation exemplified amongst abusive dropshippers in studied forums. We will fully describe how abusive dropshippers execute this abusive operation and outline how it harms customers, other sellers, and e-commerce platforms in Sec. IV.

An abusive dropshipper is located in Russia and opens a marketplace account in Amazon CA (Canada) after observing item listing gaps on the Canadian e-commerce platform and lists their chosen gap items for purchase. *Gap items* are products absent or highly priced in an abusive dropshipper's target domain but available and cheaper for fulfillment through the abusive dropshipper's source domain.

When a customer purchases from the abusive dropshipper's store in Amazon CA, the dropshipper finds a private seller to fulfill the customer's order. This private seller can be located in a different country than Canada, e.g., Amazon US, eBay US. Sourcing from outside the country allows the abusive dropshipper to easily profit as either no other seller in Canada sells the gap item, or they buy the item cheaply from a foreign private seller and list it for less than existing listings on Amazon CA. When a customer orders from the abusive dropshipper's store, the abusive dropshipper fulfills the purchase by placing an order with the private seller using the customer's address.

The abusive dropshipper, for instance, sells a popular pet toy from a US company on Amazon CA for $40 USD and fulfills customer orders from an Amazon US private seller for $22 USD (by taking advantage of Amazon's free international shipping from US to CA [11]). When a customer buys the toy from the abusive dropshipper's store in Amazon CA, the abusive dropshipper uses the customer's shipping information to purchase the toy from the US-based private seller. The private seller then ships the toy to the Canadian customer, unaware that the order comes from the abusive dropshipper.

The dropshipper repeats this process of listing (gap) items on different popular e-commerce platforms in Canada and other countries (e.g., Mexico) and aims to purchase them cheaply from unwitting private sellers to maximize total profits.

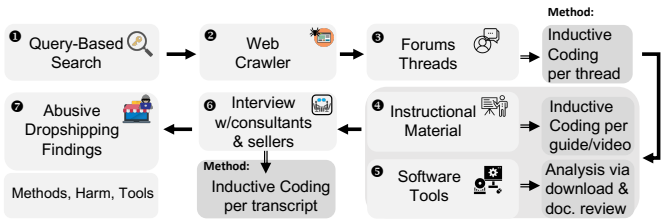

Fig. 2: Abusive dropshipping data collection process.

Abusive dropshipping vs. Gray-Market Sellers. Abusive dropshippers and gray-market resellers differ in operation, e-commerce platform regulation, and impact on customers and other sellers. By definition, *gray-market* items are "goods manufactured by or with the consent of the brand owner, purchased by a third-party seller, and sold outside of the brand owner's approved distribution channels" [48]. For instance, a gray-market seller purchases iPhones in bulk and sells them on an online platform or in their store that Apple has not permitted. Thus, gray-market sellers hold physical stock and fulfill orders without the brand owner's consent via unauthorized channels.

In contrast, abusive dropshippers do not hold physical stock but fulfill customer orders from private sellers using customer addresses. Therefore, an abusive dropshipper presents a more obscured risk to manufacturers and customers due to three reasons. They (a) sell items on an e-commerce platform with the flexibility of ordering them from different private sellers, (b) operate remotely from different countries with minimal maintenance by not holding item stocks, and (c) take advantage of gap items in different countries and fulfill those items from private sellers by exploiting the international free (or low-priced) shipping of e-commerce platforms.

III. Data Collection and Methodology

We study abusive dropshipping methods and behavior for monetization on e-commerce platforms and answer the following research questions:

RQ1 What are the abusive dropshipping methods used by sellers that violate e-commerce policies?
RQ2 What tools are used to carry out such methods?
RQ3 How do these abusive operations harm customers, other sellers, or e-commerce platforms?

Fig. 2 presents our data collection process and analysis to answer these questions. Using a query-based search, we crawled Google to discover forum threads discussing abusive dropshipping (❶ - ❸). We inductively coded threads to gain insight into abusive dropshipping operations. During this process, we discovered instructional materials (e.g., text guides and videos) and software tools used by abusive dropshippers. We analyzed instructional materials via inductive coding after reviewing text guides and viewing videos (❹). We read software documentation and locally downloaded when applicable (e.g., browser extensions) to understand their operation (❺).

We conducted interviews with consultants and sellers and inductively coded the resulting transcripts (❻). Our findings from our internet crawl and interviews help illustrate abusive dropshipping methods, tools, and harm against customers, sellers, and e-commerce platforms (❼).

TABLE I: Studied forums and instructional materials discussing abusive dropshipping.

#	Name	Details
A. Discussion Forums		
1	Reddit /r/dropship [80]	1,253 Threads
2	Warrior Forum [106]	166 Threads
3	BlackHatWorld [19]	989 Threads
4	forum.alidropship [41]	534 Threads
5	forum.donanimhaber [42]	183 Threads
6	voz.vn [103]	250 Threads
7	kaskus.co.id [57]	276 Threads
B. Online Courses and Guides		
1	Dropshipping Business Details [73]	Paid (8 Text-based Guides)
2	Dropshipping Success Stories [2]	Free (42 Text-based Guides)
3	Amazon VN [109]	Free (62 Video Guides)
4	Dropshipping Case Studies [110]	Free (24 Video Guides)

A. Forum, Instructional Material, and Software Data

To answer our research questions, we started an initial crawl of the Google search engine via a Python API [46] for dropshipping-related information. In this step, we used the queries "dropshipping" and "dropship" (and the alternative form - "drop ship") for our initial crawl. Using these queries, we collected 238 unique web pages.

Two authors read each page, labeled it benign or abusive, and found that only 24% of web pages discuss abusive dropshipping. To increase the likelihood of collecting abusive dropshipping content, authors extracted phrases for each abusive web page to supplement our query list. Authors focused on phrases that describe abusive dropshipping operations, such as "dropshipping without permission" and "dropshipping no agreement." We enriched our list with a total of 24 queries that focused on discovering *abusive* dropshipping content (See Appendix B Table VI for queries). Using this query list, we crawled the Google search engine to discover 931 web pages.

Two authors examined a random sample (20%) of returned web pages to determine if our crawler returned dropshipping-relevant content. If any dropshipping practice was discussed (e.g., discovering suppliers, choosing items to sell), authors labeled the web page as relevant. Of the randomly sampled web pages, 82% contained dropshipping-relevant content, verifying our crawler's ability to capture dropshipping content.

To curate a dataset with a high density of *abusive* dropshipping content, we sought to discover popular domains discussing the operation. We grouped web pages by their top-level domain and discovered that 40% discussed abusive dropshipping. Of this, approximately 30% comprised non-forum domains such as blog entries, news articles, and YouTube videos. We discovered that a high volume (70%) of abusive dropshipping content emerged as threads on discussion boards and online forums, which we further crawled, as detailed below.

A. Discussion Forums. Table I-A presents seven discovered popular online forums. Users on forums 1 and 4 solely discuss dropshipping, while the remaining forums contain a subgroup that discusses the operation. We note that all forums are marketed as benign yet contain a subgroup of users who discuss abusive dropshipping methods. We selected the top seven forums (by quantity) detected from our crawler run, after filtering out irrelevant forums (e.g., forum threads discussing e-commerce and only briefly mentioning dropshipping). Interestingly, forums $5-7$ involved discussion in non-English languages (Turkish, Vietnamese, Indonesian, respectively). Our crawler discovered these forums due to forum users' use of the words from our query list in their English form. The discussion of abusive dropshipping from non-English speakers is plausible due to an abusive dropshipper's ability to operate from any country. We included these forums as (1) our initial query-based crawl captures them, and (2) they provide additional insight into abusive dropshipping from non-English speakers.

After selecting relevant forums, we recrawled the Google search engine, using our query list and `site` filter, which allows returned links to be restricted to a high-level domain name (e.g., `site:`reddit.com/r/dropship/). This feature allows us to extract abusive dropshipping threads hosted on these forums. To better capture abusive dropshipping discussions hosted on Forums 5-7, we translated queries in our list to the forum's respective languages using the Python Google Translate API [47]. After deploying our crawler, which ran for ~ 114 hours, we curated a dataset of abusive dropshipping discussion consisting of 3,651 threads across seven forums.

Analyzing Forum Threads. To analyze our collected threads, we randomly sampled 30 threads for each forum (210 threads). We leveraged the Python Google Translate API [47] to translate the non-English forum threads. After sampling and translation, two authors conducted thematic analysis, independently performing inductive coding per thread. We focused on generating themes of abusive dropshipping methods, tools, and harms.

Per guidelines from prior work [82], our thematic analysis was iterative and involved multiple rounds. We continually sampled 30 threads across each of the seven forums (210 threads per round), repeating our analysis until we generated a stable codebook and reached thematic saturation. Between each round of coding, authors who independently coded threads met to reconcile differences. Authors achieved high agreement (Cohen's Kappa, $\kappa > 0.80$) before each round of coding reconciliation. We reached saturation after analyzing 1050 threads ($\sim 30\%$ of collected threads). To avoid presenting anecdotal themes, we ensure themes in our analysis are prevalent across all forums (See Appendix C-A for full codebook).

Approximately 25% of analyzed threads included discussion from sellers who allege they have been used as a source (private sellers) by abusive dropshippers. 70% of threads involved discussion amongst abusive dropshippers. We refrained from pruning/filtering via machine learning classification as only $\sim 5\%$ of threads analyzed were related to compliant dropshipping (with no mention of abusive dropshipping).

To develop a better understanding of the types of external resources used by abusive dropshippers, we noted resources referenced by forum users during our inductive coding. We discovered two groups of commonly mentioned external resources - (1) *instructional material* in the form of online courses or guides and (2) *software tools*. We further analyzed instructional material and software upon criteria that they are discussed amongst abusive dropshippers, and have a prevalence of at least 10% within any analyzed forums. We selected this threshold to ensure resources selected for further analysis were not singularities but rather have been leveraged by multiple users while also generating a diverse list of resources to analyze.

B. Instructional Material. Table I-B presents four widely-

TABLE II: Discovered software tools used by abusive dropshippers, grouped into three categories.

#	Tool Name	Type†	Details
C1. Product Research and Listing			
1	Helium 10 [50]	Chrome (900K+ users)	Free trial (+$97-$397/mo)
2	AMZScout [14]	Chrome (100K+ users)	Free trial (+$44.99/mo)
3	Jungle Scout [56]	Web	$39-$129/mo
4	Viral Launch [102]	Web	$59-$199/mo
5	AMZ Blast [13]	Chrome	$65-$175/mo
C2. Repricing and Revenue Analytics			
1	Informed Repricing [53]	Web	Monthly revenue-based
2	BQool Repricing [22]	Web	Free trial (+$25-$100/mo)
3	Aura Repricer [15]	Web	$97/mo
4	Repricer Express [81]	Web	Free trial (+$55-$249/mo)
5	Seller Engine Plus [83]	Web	Free trial (+$49.95/mo)
C3. Product Reviews and Seller Feedback			
1	Feedback Express [39]	Web	Free trial (+$23-$119/mo)
2	Feedback Genius [84]	Web	Free trial (+49-499/mo)

† Chrome is for Chrome Extension, Web is for Web-based Software.

leveraged online guides that inform abusive dropshippers on successful exploitative methods. Two of these materials comprise text-based guides such as articles (Table I-B$-1, 2$), while the remaining two guides include video media (Table I-B$-3, 4$). Two authors reviewed text-based guides and viewed video content. We employed the same technique for analyzing forum threads, performing independent inductive coding before reconciling differences to generate a codebook. For materials that required payment, we only considered free previews (visible to anyone without payment). We note that individuals who publish free guides do so (1) as previews to encourage the purchase of paid products (e.g., software) and (2) for ad-profit on content-hosting platforms. Similar to translating threads, we translated non-English text in text-based guides (Dropshipping Business Details) and viewed non-English videos (Amazon VN) with automated English subtitles. We present our codebook for our instructional material in Appendix C-B.

C. Software Tools. We discovered software from analyzed forum threads described by users as effective in facilitating abusive dropshipping (Table II). These tools are used by compliant dropshippers, but also leveraged by abusive dropshippers. We also discovered tools with malicious capabilities solely used by abusive dropshippers. To prevent supporting abusive activities, we do not include such tools in Table II. To analyze tools, we read their documentation and installed them locally (for Chrome extensions) to understand how they operate. We will discuss the role of these tools in specific scenarios in Sec. IV.

Our analysis of forum data, instructional material, and software tools shed light on how abusive dropshippers operate. We discovered abusive dropshipping operation modes involving (a) exploitative item selection, (b) volatile item fulfillment, and (c) abuse of software tools to support their activities.

These modes of operation impact customers, sellers, and e-commerce platforms, causing apparent harm to these parties. For instance, abusive dropshippers either do not provide or forge package tracking numbers when selling items to customers causing inconvenience to the customer who cannot track their shipment (Sec. IV-B). Yet, it is difficult to infer how parties are affected by more intricate abusive dropshipping methods. For instance, to avoid legal issues from selling trademarked products, abusive dropshippers source non-trademarked products. Yet, it remains not fully clear from crawled data how this tactic affects sellers of such products. Similarly, forum data may not yield insights into how sellers' perceptions of platforms are affected due to the persistence of abusive dropshippers.

To bridge this gap of how abusive dropshipping affects customers, sellers, and the e-commerce platform itself, we conducted semi-structured interviews with qualified individuals who have experience with e-commerce, detailed subsequently.

B. Semi-Structured Interviews

We collected data from two types of qualified experts: (a) consultants who provide legal and business-strategy advice to e-commerce sellers and (b) experienced e-commerce sellers who have been involved for at least two years. Our interview questions are designed to gather insights into participants' perspectives of abusive dropshipping, with follow-up questions asked based on participant answers and experiences.

Recruitment. We started recruitment via purposive sampling, reaching out to known (1) legal consultants with expertise in the domain of abusive dropshipping and (2) experienced sellers. We note that our criteria for purposively sampling sellers did not mandate any knowledge of abusive dropshipping.

We reached out to 11 individuals for initial screening. We also leveraged snowball sampling, where interviewed participants passed along our contact information to other potential candidates. In recruitment, we framed our study as a study to understand perceptions of dropshipping methods.

All potential participants underwent screening to ensure they were qualified for our study. We required all participants to (1) consult e-commerce sellers affected by abusive dropshipping or (2) be e-commerce sellers with at least two years of experience. We required participants to be above the age of 18.

Participants. We heard back from 10 individuals who expressed interest and underwent screening. Four individuals did not pass our screening test and were not invited for our interview. We recruited a total of six participants. These participants comprise four Amazon FBA sellers, one compliant dropshipper, and one legal consultant with extensive experience with e-commerce sellers. Interviewed sellers and seller clients of legal consultants operated within the United States. All participants were aware of compliant dropshipping and abusive dropshipping.

Protocol. We designed our interview protocol to understand abusive dropshipping's impact on different e-commerce parties: customers, sellers, and the platform itself. We first asked participants introductory questions (e.g., profession, involvement in e-commerce). We then outlined compliant dropshipping, asked participants about their awareness of the business model, and asked how participants perceived its impact on the different parties. We subsequently outlined abusive dropshipping. We asked participants about their awareness of the model, and whether abusive dropshipping can benefit or harm e-commerce parties. We concluded by asking participants if they had first-hand experience with abusive dropshipping and how they had been affected by it. We provide full screening and interview questions in our interview protocol [54].

For sellers, we introduced abusive dropshipping as "alternative dropshipping" (and avoided words indicating exploitation/abuse) in both screening questions and during our

interview to minimize bias. We did this to solicit sellers to discuss the overall impact of abusive dropshipping, instead of priming them to discuss harm. We also did not prompt participants to explicitly share their opinions of specific abusive dropshipping tactics. However, some participants voluntarily expressed knowledge of such tactics. We note how they support forum and instructional material finding in Sec. IV.

Our study was considered exempt by our IRB (which grants exemption to minimal-risk interviews with populations excluding pregnant women/prisoners/children). Interviews were conducted/recorded (with consent) via Zoom - each lasted 45 minutes (average). Participants were not financially compensated. Recordings were deleted after author transcription.

Interview Analysis and Findings. Two authors independently analyzed interview transcripts via inductive coding. They generated initial codes, merging similar codes under the same theme. Authors came together to reconcile disagreements after analyzing transcripts. They achieved high inter-coder agreement (Cohen's Kappa, $\kappa > 0.80$) before reconciliation. After analyzing our six interviews, we had reached thematic saturation and thus stopped recruitment. We present our codebook for our interviews in Appendix C-C.

All interviewed participants viewed compliant dropshipping as fair and beneficial, specifically attributing this characteristic to the presence of a formal agreement. This finding ensures that the effects of abusive dropshipping raised by interviewed participants specifically relate to abusive dropshipping and not the compliant dropshipping model. We note that all participants were aware of abusive dropshipping, with all five sellers noting having been used as a source of items for abusive dropshippers. We present our collective findings of abusive dropshipping impact on sellers, customers, and e-commerce platforms below.

IV. Abusive Dropshipping Operation and Impact

From analyzing various forums, software tools and interviews with consultants and sellers, we discovered exploitative behavior conducted by abusive dropshippers. Broadly, this behavior stems from two operations:

- **Abusive item sourcing** Sec. IV-A describes methods abusive dropshippers use to strategically list items for sale to avoid being flagged by e-commerce platforms.
- **Volatile order fulfillment** Sec. IV-B discusses abusive dropshippers' fulfillment of customer orders.

Additionally, these behaviors result in order return intricacies and even cause abusive dropshippers to be marked by identifiable characteristics:

- **Handling returns** Sec. IV-C describes how abusive dropshippers face complications in processing returns.
- **Strategies across marketplaces** Sec. IV-D notes how operations are designed to apply to most marketplaces.
- **Abusive dropshipping characteristics** Sec. IV-E presents identified characteristics that abusive dropshippers exhibit due to their behavior (e.g., targeting lower-priced items to minimize loss when refunds are issued).

In Fig. 3, we define qualitative terminology for attributing data source and prevalence to themes presented in the following

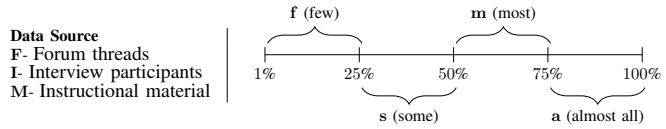

Fig. 3: Terminology for theme source (either **F**, **I**, **M**) and % prevalence (**f**:1%-25%, **s**:26%-50%, **m**:51%-75% , **a**:76%-100%).

subsections, similar to prior work [38]. We delineate between forums (**F**), interviews (**I**), and instructional material (**M**), and note percentage prevalence as one of four categories (**f**, **s**, **m**, **a**). For instance, **F:m** denotes a theme prevalent between 51%-75% (most) of threads while **M:a** denotes themes present in 76%-100% (almost all) of instructional materials.

A. Abusive Item Sourcing

After determining the platforms to buy and sell on, abusive dropshippers choose items to list in their marketplaces from private sellers. They accomplish this by manually browsing e-commerce websites and/or using dropshipping software to find *gap items*, items either not available or available for a higher price on the target e-commerce platform.

1) Gap Items: In analyzing forum discussion surrounding product choice, we uncover that abusive dropshippers have two motivations behind gap item selection: (1) exclusivity-motivated gap items, and (2) competitive profit-motivated.

Exclusivity Items [F:a, I:s, M:a] For exclusivity-motivated gap items, an item is unavailable to customers on the abusive dropshipper's target platform but available on their source platform. For instance, customers in Canada and Mexico may desire popular items sold in the US that are unavailable in their home country. Similarly, an abusive dropshipper uses private sellers in Japan to sell items to Japanophile communities in the US and Europe. Here, the abusive dropshippers exploit the target platform item *unavailability* that exists due to vendors not yet selling an item in a region. Electronics, kitchen appliances, and clothing are the most frequently mentioned exclusivity item categories in our analyzed forums.

These exclusive items are sold for a much higher price than those listed by the private seller. For instance, one interviewed participant noted *"[abusive] dropshippers list items for 3 times the original price."*. An unreasonable increase is unfair to customers who have to pay a high markup to obtain an exclusive item that is otherwise unavailable to them on the *target* platform.

Abusive dropshipping's price markup occurs at a much larger scale than traditional reselling. This is due to abusive dropshipping's ability to not hold stock and operate without a physical presence. Interestingly, interviewed participants also note how the price markup can introduce long-term harm: a source merchant's reputation and brand image are damaged. Although a product's origin may be unknown to buyers, markups cause a mismatch in expected quality (more expensive items are assumed to be of higher quality). Thus, unsatisfied buyers post poor reviews on external forums. Potential buyers who preview these forums are disincentivized to purchase from source merchants carrying the same brand. For instance, one participant stated *"when a customer buys a 50 dollar item, they expect the item to be of that quality - however, they get the*

quality of a 10 dollar item", with another noting an experience where a quality-price mismatch caused *"the seller's brand to receive very bad comments and reviews in online forums. So the seller loses their reputation."*

Competitive Profit Items [F:a, I:s, M:a] Competitive profit motivated gap items are sold by the abusive dropshipper on the target platform for less than the existing listings of the same item from other sellers. For instance, consider a baby product, e.g., milk bottle, with the lowest list price on the abusive dropshipper's target platform (e.g., Amazon MX) of $302 MXN (~$15 USD). The abusive dropshipper identifies this as a competitive profit-motivated gap item since a private seller in Amazon US sells the same bottle for $7 USD with free international shipping. The abusive dropshipper lists this item on the target platform for $242 MXN (~$12 USD), netting a $5 USD profit per Amazon MX customer purchase. Abusive dropshippers find successful margins leveraging competitive profit items. For instance, one forum user selling such items in a Mexico-based operation noted that *"in a month I was able to bank 10k... a 40% margin, so pretty good numbers."*

2) Trademarked and Non-Risky Items: Apart from profit and exclusive gap items, we discover that abusive dropshippers consider the trademark status of items, criteria important to ensure the longevity of their operation and continuous profit.

Avoiding Trademarked Items [F:a, I:a, M:a] Our findings show that abusive dropshippers avoid listing items that are trademarked. They note that selling trademarked items usually results in these listings being removed by the platform. One interviewed participant stated that *"even if the platform [does not] remove the listing [of a trademarked item] immediately, they usually remove it after the seller's 3rd/4th sale after the trademark owner makes a complaint."*

While abusive dropshippers may list items from more prominent larger brands (e.g., General Electric, KitchenAid, Adidas) with registered trademarks, these companies quickly report and take action against sellers, reducing the longevity of the abusive dropshipper's store. One interviewed participant stated, *"If the seller is selling Adidas or Nike or you know, like the big brands, [Amazon] will check. But if the seller is selling small brands, they do not really check."*

To prevent this from happening, sellers opt for brands that are not trademarked. Abusive dropshippers refer to such items as *"non-risky items,"* noting success in listing these items without any issues, detailed in the following subsection.

3) Operating via Underground Collaboration: We observed that abusive dropshippers collaboratively construct aggregated item lists. They leverage prior experience to identify (1) non-risky items and (2) profitable gap items.

Non-risky Item Discovery [F:s] We discovered efforts to aggregate brands that abusive dropshippers may infringe on with a low risk of account suspension (higher-risk brands are known to file reports to e-commerce platforms, which trigger suspension of abusive dropshippers' accounts due to violation of terms of service). For instance, one discovered list contains an extensive, frequently updated *allow list* of non-risky brands to filter items, compiled in a Google Sheets document. A note at the spreadsheet's header described it as *"...a list of non-risk brands that have been successfully sold without issue, as reported by our users."* Abusive dropshippers leverage this document for malicious product research.

TABLE III: Sample records for items in the uploaded data.

Item†	Date Added	Initial Price ‡	Sale Price *	Target
BMR Bluetooth Adapter for Bose SoundDock	05/11/2018	$26.18	$46.36	Mexico
Hot Wheels Star Wars Stellar Vehicle Toy	01/22/2019	$11.61	$29.75	Mexico
Manchester City FC - EPL Knit Scarf	03/30/2019	$25.69	$57.51	Mexico

† Translated from Spanish, ‡ Private Seller Item Price on Amazon US, * Item Listing Price on Amazon MX (All prices are converted from MXN to USD).

At the time of our viewing, we observed multiple users contributing to this list and 2,814 rows of unique brands. Using this technique, abusive dropshippers ensure the longevity of their operations, evading reports stemming from many major item listings and continuing to operate in popular marketplaces.

Synergy to Identify Profitable Gap Items [F:s] We additionally find that abusive dropshippers collaborate to coalesce profitable gap items. Here, they leverage the knowledge of successful abusive dropshipping operations to outline gap items proven to have demand among customers in a target domain (which abusive dropshippers often dub "winning products"). Requests to gain access to such lists are common, e.g., *"Does anyone have a list of products that are currently selling a lot with dropshipping... would be very grateful."*

To understand the selection of profitable items, we present a widely referenced compilation of gap item records posted in one of our analyzed forums (via a link to `PasteFS` [74]). This data presents an abusive dropshipping community-collaborated list of US items to sell on MX; users leveraging this list claim successful operations. Further validating these records, insights from this data complement our forum findings by further supporting abusive dropshipping trends, noted below.

This popular aggregate of successful gap items comprised 4,411 items listed over 15 months from Amazon MX, where the purchases can be fulfilled from various Amazon US private sellers. Notably, selling items in Mexico while fulfilling customer orders from a private seller in the US, without formal agreements with suppliers, corresponds to abusive dropshipping.

Table III illustrates three sample gap items in the data dump. Each data point contains (a) Listing Name, (b) Timestamp of Item Added, (c) Private Seller Item Price on Amazon US, (d) Item Listing Price on Amazon MX, and (e) Target Platform (Mexico). For example, the item "Hot Wheel Star Wars Stellar Vehicle Toy," added on January 22, 2019 for $29.75 USD on Amazon MX, can be fulfilled from an Amazon US private seller for $11.61 USD, providing the abusive dropshipper a potential revenue of $18.14 USD (a 156% increase).

Overall, the items in the data dump have an average listing price of $\$43.70 \pm 19$ on Amazon MX. Comparatively, the operation supplies items from Amazon US private sellers for an average price of $\$21.40 \pm 10.20$ USD (including shipping), resulting in a 104% average price increase.

Fig. 4 shows the item prices and the number of items in the gap item records. The CDF reveals 90% of items had a price

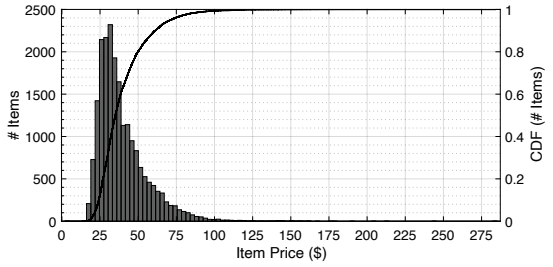

Fig. 4: Item listing prices in Amazon MX vs. the number of items (with the CDF plot).

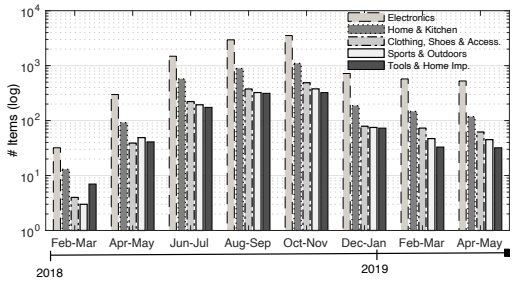

Fig. 5: # of items for the most popular five categories grouped by item addition date in the gap item records.

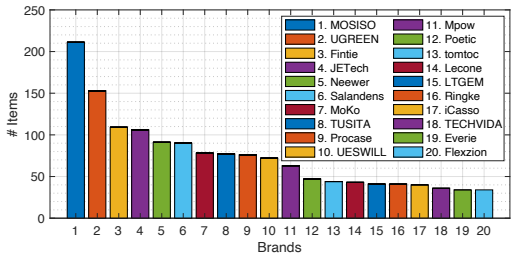

Fig. 6: # of items for top 20 brands in gap item records.

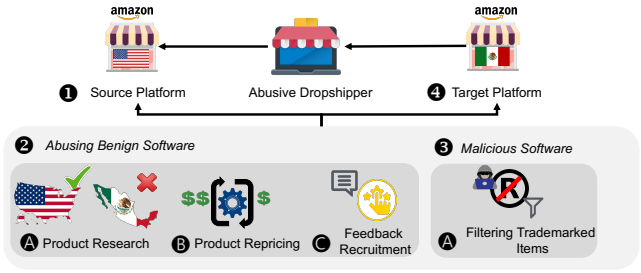

Fig. 7: Item selection facilitated by benign and malicious software. We use MX and US as examples of source and target platforms (software used to target other regions is prevalent).

less than $61.09 USD. Although we are not able to infer what type of gap items (exclusive or profit-motivated) were involved in this operation, we note that the average 100% price increase supports the strategy of unfair markup with exclusive items.

In Fig. 5, we plot the number of items in the top five categories in two-month periods based on item addition dates. The category with the greatest quantity of items is "Electronics" followed by "Home & Kitchen" (two popular exclusive gap items mentioned in Sec. IV-A). The variety of items (shown in Table III and Fig. 5) and the lower price are consistent with abusive dropshipping behavior, discussed in Sec. IV-E.

Lastly, in Fig. 6, we present the number of items found in the top 20 brands in the records. All top 20 brands are lesser-known, such as Mosiso, Ugreen, and Fintie. These brands are considered *"non-risky"* by abusive dropshippers, complementing forum findings (e.g., *"Best to stick to items that are unbranded or some weird [country] brand"* to prevent *"anyone [from] sue[ing] or shut[ting] down [your] website"*).

Persistence via Forged Documents [F:f, I:s, M:f] Despite noted success with non-risky items, abusive dropshippers may face scenarios where a brand owner files a complaint against the abusive dropshipper. In response, the *target* domain prompts the abusive dropshipper for proof that they have permission to sell listed items (i.e., Letter of Authorization letter).

Echoing instructions in online guides and forum findings, we found evidence from interviewed participants that abusive dropshippers forge "Letter of Authorization" documents to overcome this issue, causing private sellers' complaints to be dismissed by e-commerce platforms. For instance, one interviewed participant stated that when reaching out to e-commerce platforms to report a suspected abusive dropshipper selling their items, *"the platform said [the dropshipper] has [fake] documents although I confirmed with the manufacturer that I am the sole distributor in [region]."*

Complementing this issue, we found a prevalence of resources in forums/instructional materials promoting the forgery of such documents. For instance, an instructional video has a section titled *"How to circumvent License of Authorization on Amazon (Sample License of Authorization Text)"* with a sample license document to send to an e-commerce platform.

In the event that the private seller of the non-risky item successfully removes the abusive dropshipper's listing, the abusive dropshipper updates the collaboratively constructed *allow list* document, noting that the non-risky item has documented cases of complaints. This process helps other abusive dropshippers not to fulfill customer orders from this seller or list the same item. The abusive dropshipper then proceeds to source the same or similar item from different private sellers to continue their business.

4) Exploitative Use of Dropshipping Software: We studied both benign and malicious software that provide abusive dropshippers with capabilities for exploitative item selection. Fig. 7 presents how these software tools facilitate selecting items from a source platform (❶). Studied software, in Table II, are not malicious in nature. However, abusive dropshippers exploit these benign software tools (❷) to filter and identify potentially profitable gap items from different private sellers via product research software and ensure these gap items stay profitable via repricing/product feedback software (Ⓐ-Ⓒ).

Abusive dropshippers also leverage software tools that are advertised with malicious capabilities. Malicious tools (e.g., `Software-Mal`[3]) complement gap item filtering of

[3]Anonymized as it is marketed for abuse - available for research on request.

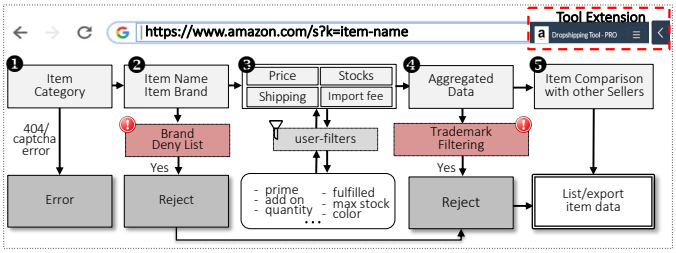

Fig. 8: Reverse engineered execution flow of malicious dropshipping tool (`Software-Mal`), a subscription-based product research & listing tool designed for abusive dropshippers.

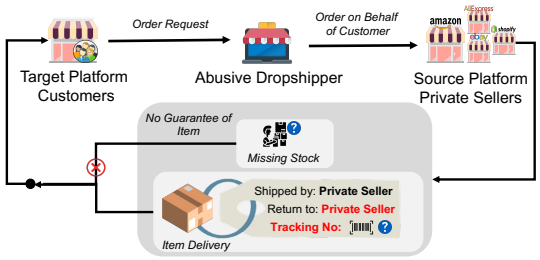

Fig. 9: Fulfillment process used in abusive dropshipping.

benign software with additional features and include additional community-driven functionalities (e.g., filtering trademarked items, ❸) to help abusive dropshippers circumvent platform regulations and persist in target marketplaces (❹).

Abusing Legitimate Software [F:a, M:a] Product research software is typically abused to discover gap items, while repricing and review software are used to ensure gap items are attractive to customers. For instance, product research software with geographic filtering allows abusive dropshippers to quickly identify multiple private sellers from which they can find profitable gap items (supported by all tools in **C1**-Table II). Abusive dropshippers first specify their source e-commerce platform, selling platform domain (e.g., Amazon US and Amazon MX), and a number of broad item keywords (e.g., computer mice, office chairs, cooking utensils). The software performs automated queries using the keywords to the target e-commerce platform, outputting gap item products.

Similarly, abusive dropshippers use benign repricing tools for strategic pricing (supported by all tools in **C2**-Table II). Such tools compare an abusive dropshipper's product listing price with the lowest price offered in the market. If a different party offers a lower price, it updates the dropshipper's product listing price. Here, abusive dropshippers use repricing tools to continuously confirm that selected gap items are priced competitively while ensuring profit.

They also use benign product review/feedback software (supported by all tools in **C3**-Table I). Such tools periodically prompt customers to submit positive product reviews and feedback (e.g., rating the item and seller). Abusive dropshippers use such software to request customers to provide 5-star reviews for their gap items. Positive public feedback incentivizes customers to purchase these gap items from dropshippers.

Software Marketed for Malicious Use [F:m, M:m] To illustrate how malicious software can be (ab)used to *strategically* find items while avoiding trademarked items, we present the execution flow of `Software-Mal` on Amazon in Fig. 8, discovered in analyzed threads. This tool is marketed as *"quickly [to] integrate into your browser, access hundreds of product lists within minutes and upload them to ... with a single click."* `Software-Mal` is similar to "Product Research and Listing" software in Table II, streamlining the process of optimizing product search but with additional capabilities.

To begin the analysis of `Software-Mal`, we locally installed it and hooked into its execution by adding breakpoints through Chrome's built-in DevTools. This allowed us to iteratively explore the chain of execution for parsing of item pages, and discover any logic (e.g., internal functions, API calls) performed. `Software-Mal` crawls the listing page of each item from a user-submitted item category query, collecting an item's name and brand while filtering out brands specified in a user-maintained brand denylist. This denylist comprises brands that have filed complaints against abusive dropshippers and are updated when new complaints are received (❶, ❷).

`Software-Mal` next collects an item's price, shipping cost, Amazon Prime status (❸), and marketplace/seller-specific information (e.g., count and current stock of other sellers listing the item). At this point, optional secondary item filtering based on trademark status (❹) can be performed. Here, the tool's *trademark filtering* makes requests to public services `Bulk-SEO-Tools` [23] and `Trademarkia` [99], obtaining a CSV file of crawled item brands' trademark statuses and passes items whose brands are trademarked to the "Reject" function. Abusive dropshippers use this option to extend operation longevity, avoiding established brands likely to report any infringing listings, but taking advantage of sellers that may not be able to trademark their products/brand.

Lastly, `Software-Mal` performs a final filter on collected items to minimize listing competition (❺). To do so, `Software-Mal` uses items' Amazon Standard Identification Number (ASIN), a ten-character sequence constant across all Amazon domains that represents an item, to form URLs for items and pings these addresses. If the page exists, another seller currently lists the same item in the target domain, indicating competition. `Software-Mal` saves the results of these various filters in a CSV file for manual inspection by the user.

B. Volatile Item Fulfillment

After a customer places an order from the abusive dropshipper's e-commerce store, the abusive dropshipper fulfills this purchase. Fig. 9 presents the fulfillment process and the issues that customers face in tracking and receiving their orders.

1) Item Shipment: Since the seller is an abusive dropshipper, no formal agreement is established with the private seller. When a customer orders from their store, the abusive dropshipper fulfills the purchase by ordering from the private seller using the customer's address. The return address on the item packaging is that of the private seller, as it is the private seller who ships the order unaware of the abusive dropshipping operation.

Withholding Shipment Information [F:s, I:m] Once the order is shipped, the abusive dropshipper gets access to the tracking number (provided by the private seller). However, we

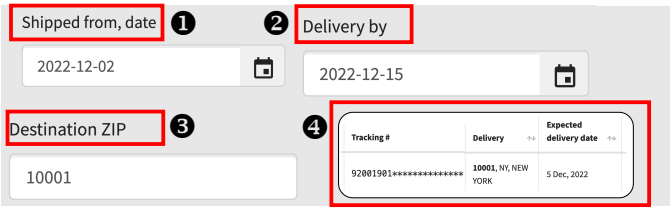

Fig. 10: The software accepts the following inputs - ❶ ideal shipped date, ❷ ideal delivery deadline, ❸ destination zip code - to output ❹ candidate tracking numbers.

find that abusive dropshippers withhold information about an order from customers. Specifically, abusive dropshippers prefer not to provide tracking numbers to customers for two reasons.

First, we found from studied resources that when an abusive dropshipper provides the tracking number from a private seller, e-commerce platforms suspend their accounts. This is because the target platform identifies a discrepancy since the items are shipped to customers from a different region than the abusive dropshipper's listed address on the target platform.

Second, abusive dropshippers who operate outside the country of their target platform note that including tracking numbers may raise suspicion from customers. This is because the customers do not expect their tracking number to display a foreign country as the source of the package. For instance, a user orders from an e-commerce platform in MX, but the tracking details of their order show the order is coming from another seller in a different country. An abusive dropshipper in our forum data justified their decision to avoid tracking numbers, stating *"if customers know the products come from [outside where I am], I'll lose credibility."*

We note that this lack of information is intrinsic to abusive dropshippers as compliant sellers/dropshippers have no incentive to withhold tracking numbers. Withholding information harms customers who do not receive full transparency about their orders. One interviewed participant notes abusive dropshippers *"do not provide tracking numbers, and it is very problematic for [customers]. This is because, for international shipping, there are [many] transfer points, and the item can get damaged. [There is no] transparency for the customer to know when an item will come."*

Generating Fake Tracking Numbers - [F:f, I:f] When e-commerce platforms require sellers to provide tracking numbers, we found abusive dropshippers generate invalid/fake tracking numbers through tracking information services such as BlueCare Express [21] and packtrack [72]. Here, the abusive dropshipper may associate an order status with a "fake tracking number" which they set with reference to the original Tracking Numbers. The "fake tracking number" could be a number that the abusive dropshippers have full control over (e.g., manipulate status such as shipped, out for delivery, or delivered). However, it could also be an existing tracking number that is associated with a random order. Fig. 10 provides an example software that returns candidate tracking numbers that satisfy the input delivery deadline, shipment date, and destination zip code.

Our forum data exposes how such services have exploited customers. For instance, one Amazon customer detailed that a suspected abusive dropshipper *"...provided a false tracking number for a myhermes parcel. It was not delivered. Myhermes confirmed the tracking info, is for a different address"* suggesting that the abusive dropshipper had provided a random tracking number associated with a parcel in the same region. Another forum user who purchased from a suspected abusive dropshipper stated, *"Bluecare [service is] saying [my] item [was] delivered to letterbox. It was not delivered. It is a small value item that has been bought from a UK eBay seller and supposedly shipped by a US company. Highly suspicious !!"*

2) Lack of Item Guarantee: As abusive dropshippers run their operations without formal agreements, they have no control over or guarantee of physical stock for items they list. For instance, an abusive dropshipper who receives an order of 20 phone cases from a customer has no guarantee that the private seller will have sufficient stock. This leaves an abusive dropshipper's customers with no guarantee of item fulfillment.

Procrastinating or Neglecting Orders - [F:s, I:m] Due to stock uncertainties, customers are also continually harmed by abusive dropshippers' method of fulfillment. If an item listed by an abusive dropshipper is not in stock at any private seller, the abusive dropshipper will either stall for stock or ignore the order. This forces the customer to exert additional effort communicating with the e-commerce platform and experience delays. We note that abusive dropshipping poses a heightened risk of this harm compared to compliant sellers. Contrary to abusive dropshippers, compliant sellers are guaranteed stock and have a full overview of existing stock as they either manage their stock or have contracts with suppliers.

While the e-commerce platform may handle such complaints through guaranteed delivery policies, the inconvenience and potential fraud introduced by the abusive dropshipper are detrimental to the customer. For instance, the following review was left on the account of an abusive dropshipper, as alleged by an Amazon community member: *"The product never arrived [and they asked me to] wait for two and a half months. Terrible customer service [and] no effort to refund or communicate with [me]."* To combat negative reviews, abusive dropshippers solicit fake positive reviews (e.g., *"Does anybody sell fake [platform] reviews?"*), in an effort to boost store image and minimize the impact of organic negative reviews on their store.

We note that interviewed sellers raise fulfillment inconvenience as an issue that affects private sellers. This is because on some platforms (e.g., Amazon), customers are allowed to "rate" the product itself and not the seller. Low ratings due to an abusive dropshipper cause the same product available via the original seller's store to have a low rating. One interviewee stated, *"the customer who does not receive the product may not know how to rate the seller, and instead rates the product"*, causing *"my own product to be [perceived] negatively."* Other interviewed participants note similar concerns, especially when the products they list are manufactured by the seller themselves. One participant states that *"when manufacturing own material, improper customer service such as inability to receive the order quickly may harm the brand image."*

Volatile item fulfillment can also affect the original seller's reputation. One participant noted how customers dissatisfied with an abusive dropshipper's delay can impart negative reviews on a brand (on the platform/external forums). *"[They] write*

TABLE IV: Discovered characteristics that are associated with abusive dropshippers.

#	Seller Attribute	Abusive Dropshipper Preference‡	Sample Quote from Forums
a_1	Item Categories	Variety in categories (e.g., Electronic, Home) listed (a)	*"I've [sourced] lots of product [to see] what folks are looking at and niche based on demand. "*
a_2	Items per Brand	Minimizing dependency on specific brand listings (s)	*"list [from] ... different brands, ... you can sell to more [people] and keep selling if some items get suspended."*
a_3	Brands Offered	Sourcing from many non-trademarked brands (a)	*" don't dropship trademarked items. only stick to no-brand or lesser-known brands."*
a_4	Location	Operating from a different location than targeted market (s)	*"I don't have a US address .... I will only dropship in the USA my products"*
a_5	Prices of Items	Lower priced items are preferred (s)	*"Find a cheap product on [platform]... That's the model."*

‡ We note the prevalence of themes within forum threads in parenthesis (we note, in our codebooks, when interviews and instructional material support these characteristics).

comments [the product] came to me in 30 days, this is a terrible business ... the review goes to the product." It can also introduce long-term harm to the e-commerce platform itself. Negative experiences from customers can cause harm to propagate to the platform, with customers choosing to patronize an affected platform less frequently, impacting its traffic.

C. Handling Returns

When an item is successfully shipped to a customer, an abusive dropshipper may face requests to return an item (e.g., due to the customer not being satisfied with the product).

Inconvenience during Returns [F:f, I:m] Handling returns may inconvenience an abusive dropshipper for one of two reasons. First, the return address listed on the item packaging is that of the private seller. If a customer were to return the package based on the address provided on the shipment, the dropshipper is inconvenienced as the returned product is sent to the private seller. Second, even if the abusive dropshipper could instruct the customer to return the item to the abusive dropshipper's chosen address, the abusive dropshipper may face inconvenience (e.g., not being physically present in that location or not having a location to store the returned items).

One interviewed participant detailed how abusive dropshipping operations face issues with returns. In this scenario, the abusive dropshipper was in a country outside the *target* domain's region of service, stating *"the dropshipper doesn't have a return place [and was in] another country. If the customer wants to return it, the seller has to pay too much money. Because Amazon doesn't pay for the return. And he has to send with shipping. And international shipping is super expensive."* For these reasons, abusive dropshippers prefer to provide a full refund when receiving a return request, allowing the customer to keep the item. This choice is out of necessity and motivated by the abusive dropshipper's need to continue their operation without receiving negative reviews and prevent the buyer from reporting the seller to the e-commerce platform.

D. Strategies Across Marketplaces

Our thematic analysis exposes that abusive dropshippers target popular platforms with large customer bases to increase their profit (e.g., Amazon, eBay). They allege that *most* platforms enact common countermeasures to curb abusive dropshipping activities. These include (a) tracking number verification, (b) requiring a letter of authorization documentation, (c) trademark filtering, and (d) relying on user reporting. To overcome them, abusive dropshippers have *generic* solutions to evade these countermeasures - using fake tracking number services, forging letters of authorization, avoiding trademarked goods, and soliciting fake positive reviews.

Although marketplaces may enforce unique countermeasures against abusive dropshipping activities, this information is withheld from the public; thus, abusive dropshippers do not discuss evasion unique to specific marketplaces. Abusive dropshippers also allege that smaller platforms loosely enforce countermeasures (e.g., Craigslist, Flipkart); however, they are not popular target platforms due to their smaller market share.

E. Abusive Dropshipping Characteristics

We identified five abusive dropshipping characteristics that result from behavior to ensure operation longevity (a_1 - a_3), convenience and profit (a_4) or minimize loss (a_5). Table IV presents seller attributes that relate to the characteristics we discover. These attributes are public information, and customers can observe them by visiting a seller's storefront and brand listing page. When aggregated, discussion of characteristics is prevalent in almost all (a) forum threads, with individual characteristics having a minimum prevalence of some (s).

Item categories (a_1), items offered per brand (a_2), and brands offered (a_3) define preferences for a seller's item categories and brands. We found that abusive dropshippers prefer listing items from *many categories and brands* but have *few listings* per brand. For operation longevity, abusive dropshippers use software to *filter out* items from *trademarked brands* to prevent suspension or account closure resulting from infringement complaints. This results in the listing of many non-trademarked brands. One forum user reported that *"...[at] first I sold trademarked items [but] received an account suspension. You can sell a few trademarked items but it's better to sell non-trademarked items (you can use some tools to find)."*

This strategy increases abusive dropshippers' sales by catering to a broader customer base and isolates platform delistings to specific items. Compliant sellers, conversely, select a niche product, often listing items from a few categories/brands but having many listings per brand.

Location (a_4) describes the geographic locality and validity of a seller's address. From our studied resources, we found that abusive dropshippers often operate from a different country than the marketplace they sell on to target specific consumers. For instance, instructional materials from non-English communities in our studied resources mention, *"...you can boost sales and make more money by selling in locations that aren't as saturated by other sellers."* Conversely, compliant sellers have a local (business) address to handle item shipping and returns.

Prices of items (a_5) describes the item price of sellers' listings. The business model of abusive dropshippers involves listing a *high number of items* at *low prices*. The lower-priced items pose less risk for trademark complaints and are less likely

to be returned by customers. Although, abusive dropshippers may have different thresholds of what a low price is depending on the product category and how much risk they are willing to take. If a customer requests a return, abusive dropshippers lose less money with lower-priced items (as they do not accept returns and allow customers to keep the item).

Although our qualitative analysis informs us of abusive dropshipping characteristics, further investigation is required to determine their eligibility in automated efforts to detect abusive dropshippers, discussed in detail in Sec. V.

V. Discussion and Limitations

A. Key Takeaways

We discover abusive dropshippers (1) list gap items and provide fake tracking numbers for customer satisfaction, (2) identify multiple private sellers to fulfill customer orders timely, and (3) list cheap products so customers can keep items when they desire a refund. They also collaborate to find items for listing that minimize reports of intellectual property infringement and leverage legitimate tools to get positive reviews. Such strategies allow abusive dropshippers to persist in marketplaces and continue their abusive operation.

Automated Detection of Abusive Dropshippers. We present in Sec. IV-E five abusive dropshipping characteristics obtainable from a seller's marketplace profile. Using these characteristics, a supervised or unsupervised ML model could be trained to detect abusive dropshippers. Yet, our qualitative data cannot inform concrete quantitative trends (e.g., median price of an item) or statistically significant differences between abusive dropshippers and compliant sellers in these features; both of which are necessary for training and assessing model accuracy.

Further investigation is required to determine if these characteristics are suitable features for a detection model. Such an investigation poses two main challenges. First, it requires a ground truth labeled dataset of sellers marked as abusive dropshippers or compliant, access of which can only be disclosed by e-commerce platforms. Second, if an automated detection model is feasible, an adaptive abusive dropshipper who knows the model attributes can operate their store such that they are erroneously labeled as a compliant seller, evading detection. Future work will investigate the feasibility of platform collaboration and an automated detection model.

Role of E-commerce Platforms in Mitigation. E-commerce platforms have access to the public attributes of abusive dropshippers, and additional private attributes (e.g., payment methods, and supply chain data). This information would allow connections to be drawn between abusive dropshippers' source vendors and consumers for detection. For instance, sellers' customer purchase addresses in one domain (e.g., Amazon MX) could be cross-referenced with the shipping addresses of orders fulfilled by sellers on other platform domains (e.g., Amazon US) to confirm if the MX seller is an abusive dropshipper fulfilling items through US private sellers.

This method works when the target and source platforms are from the same e-commerce platform (e.g., Amazon MX and US), as the platform has access to both shipping addresses. Yet, abusive dropshippers implementing unconventional selling methods (e.g., listing on Mercado Libre [a popular e-commerce platform operating in Latin America] and fulfilling from private sellers on Amazon US) require platforms to share transaction records. Additionally, this method would be ineffective in identifying abusive dropshippers that sell through their own e-commerce websites. Future work will explore the potential of (1) combining our findings on abusive characteristics with private attributes provided by e-commerce platforms and (2) its corresponding feasibility for identifying abusive dropshippers.

We also propose that e-commerce platforms should design countermeasures that consider input from original sellers who are victims of abusive dropshipping. First, marketplaces should provide sellers with an interface to specifically report customers suspected of abusive dropshipping (e.g., customers who place orders to multiple different addresses, suggesting an abusive dropshipping operation). Similarly, platforms could flag orders (via warning labels) from such customers, while still providing original sellers autonomy over fulfillment decisions. This would preemptively prevent abusive dropshippers from abusing the original seller. Marketplaces should also streamline post-report procedures. For example, interfaces should accommodate updates of an original seller's report (e.g., status of verifying alleged abusive dropshipper's letter of authorization).

B. Limitations

A limitation of our study is that we are unable to measure the ground-truth prevalence of abusive dropshipping on popular marketplaces. Such an effort would require internal e-commerce information, which is outside our scope. For ethical reasons, we also do not pay for abusive dropshipping materials. Additionally, given that dark and deep web content is hidden from search engines and that we would need to impersonate abusive dropshippers to infiltrate their private communities, we leave ethical protocol design to crawl them to future work. These limitations constrain our initial findings to discussion from abusive dropshippers and scenarios alleged by victim sellers of abusive dropshipping, expressed on public forums. However, we enrich our findings by conducting interviews with relevant participants (sellers and consultants).

Second, to analyze non-English content, we leverage translation via an API [47]. The automated translation may not be able to accurately translate intricacies within forums, such as forum jargon. However, we conducted our best effort to minimize this concern - we only generate codes for sentences that are fully comprehensible. Additionally, findings from non-English forums/material align with those of English forums/material, suggesting reliability of our automated translations.

We also note that our interview participants skew US-centric operations. Although we translated queries into non-English languages, our search mainly focuses on English-centric content. Thus, forum/interview data may miss intricacies relating to operations outside the US/non-English-speaking regions. Further work is required to understand intricacies that may arise from abusive dropshipping operations conducted in different target and source domains, in different regions, and how these intricacies may influence abusive dropshipper tactics.

VI. Related Work

Dropshipping has been studied as an e-commerce supply chain management strategy [1], [59]. However, such assessments focus on compliant dropshippers, who maintain formal

agreements with manufacturers to act as authorized entities. Several existing works compare the performance of various inventory and distribution channel strategies, including dropshipping [108], [30], [112], [24], [52], [44]. Other works examine the application of dropshipping strategies over traditional mechanisms [61], [75]. In contrast, we focus on how dropshipping can be exploited to execute abusive selling operations.

The security community has long analyzed underground marketplaces and forums to examine the connected economies of these entities. One line of research has examined public IRC channels, social networking sites, and underground forums for illicit or abusive activities (e.g., credit card fraud [77], [91], exploiting platform monetization [26], identity theft [18], [20], [76], denial of service tools [17], [65], spamming [97], [43], [62], SIM farms [105] and phishing [96], [70], [58], [97]). Anonymous marketplaces have also been examined for commodities (e.g., banned substances), revenues [25], [101], forum users' interactions [93], and language/culture [111].

Recent work describes concession abuse, a method in which customers abuse e-commerce merchants' return policies to obtain a refund or duplicate item while keeping the original [92]. This exploit varies from abusive dropshipping, as it only involves the victim seller and the malicious customer. Reshipping scams [49] also differ from abusive dropshipping, as scam actors exploit misinformed 'drops' who sign up to unknowingly aid the malicious reshipper in selling received items on the black market. In contrast, abusive dropshipping victims are other e-commerce sellers, the platform, and customers. To the best of our knowledge, this work is the first study that explores fraudulent dropshipping on e-commerce platforms.

VII. Conclusions

We present the first study on the characterization of abusive dropshipping on e-commerce platforms, and detail how abusive dropshippers affect consumers and compliant sellers. We accomplish this by examining diverse online e-commerce communities, and software used by abusive dropshippers and also through interviews with consultants and sellers. Our findings uncover that dropshipping can be abused, resulting in harm affecting other sellers and customers. We use this knowledge to identify five abusive dropshipping characteristics that are associated with online seller attributes. Our work highlights the significant harm abusive dropshippers pose to all parties in e-commerce marketplaces while motivating future work to develop safeguards to protect users from these risks.

Acknowledgment

We thank our anonymous reviewers and shepherd for providing us with valuable feedback that helped improve our paper. We would also like to thank the interview participants for their generous time and contribution to our research. This work is supported by startup funding from Purdue University.

References

[1] N. A. Agatz, M. Fleischmann, and J. A. Van Nunen, "E-fulfillment and multi-channel distribution–a review," *European journal of operational research*, 2008.

[2] "Dropshipping success stories," https://alidropship.com/blog/success-stories/, 2023, [Online; accessed 13-January-2023].

[3] "Aliexpress guideline," https://sell.aliexpress.com/zh/__pc/wndWNPOpMi.htm, 2023, [Online; accessed 15-February-2023].

[4] "Our seller-guaranteed services," https://sale.aliexpress.com/__pc/buyerprotection-seller_guaranteed.htm, 2020, [Online; accessed 11-March-2023].

[5] "About fulfilled by amazon," https://www.amazon.com/gp/help/customer/display.html?nodeId=201910460, 2020, [Online; accessed 13-January-2023].

[6] "Drop shipping policy," https://sellercentral.amazon.com/help/hub/reference/external/201808410, 2020, [Online; accessed 11-March-2023].

[7] "Amazon is hung up on the problem of drop shipping," https://www.ecommercebytes.com/2021/05/16/amazon-is-hung-up-on-the-problem-of-drop-shipping/, 2021, [Online; accessed 17-January-2023].

[8] "Report a violation of selling policies," https://sellercentral.amazon.com/gp/help/external/200444420, 2021, [Online; accessed 17-February-2023].

[9] "Amazon is fighting against laws that could force it to verify third-party sellers' identities and give out their contact information," https://www.businessinsider.com/amazon-lobbying-third-party-seller-transparency-laws-inform-acts-2021-6, 2021, [Online; accessed 17-January-2023].

[10] "Amazon canada guideline," https://sellercentral.amazon.ca/help/hub/reference/external/G201808410, 2023, [Online; accessed 15-February-2023].

[11] "Amazon international free shipping," https://www.amazon.com/gp/help/customer/display.html?nodeId=GY48Z9B62JLTAQV2, 2022, [Online; accessed 13-January-2023].

[12] "Amazon usa guideline," https://sellercentral.amazon.com/help/hub/reference/external/201808410, 2023, [Online; accessed 15-February-2023].

[13] "Amz blast," https://www.amzblast.com, 2020, [Online; accessed 11-March-2023].

[14] "Amzscout," https://amzscout.net/, 2020, [Online; accessed 11-March-2023].

[15] "Aura," https://goaura.com/, 2020, [Online; accessed 11-March-2023].

[16] "The hustlers making millions from goods they never handle published," https://www.bbc.com/news/technology-53759932, 2022, [Online; accessed 15-February-2023].

[17] R. Bhalerao, M. Aliapoulios, I. Shumailov, S. Afroz, and D. McCoy, "Mapping the underground: Supervised discovery of cybercrime supply chains," in *APWG Symposium on Electronic Crime Research (eCrime)*, 2019.

[18] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in *International Conference on World Wide Web*, 2009.

[19] "Blackhatworld," https://www.blackhatworld.com/, 2023, [Online; accessed 13-January-2023].

[20] J. Blocki, B. Harsha, and S. Zhou, "On the economics of offline password cracking," in *IEEE Symposium on Security and Privacy (S&P)*, 2018.

[21] "Bluecare public tracking facility." https://www.bluecare.express, 2020, [Online; accessed 11-January-2023].

[22] "Bqool," https://www.bqool.com/, 2020, [Online; accessed 11-March-2023].

[23] "Trademark search. bulk check trademark of 500 names," https://www.bulkseotools.com/bulk-trademark-search.php, 2020, [Online; accessed 13-January-2023].

[24] W. Chiang and Y. Feng, "Retailer or e-tailer? strategic pricing and economic-lot-size decisions in a competitive supply chain with dropshipping," *Journal of the Operational Research Society*, 2010.

[25] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *International Conference on World Wide Web*, 2013.

[26] A. Chu, A. Arunasalam, M. O. Ozmen, and Z. B. Celik, "Behind the tube: Exploitative monetization of content on {YouTube}," in *USENIX Security*, 2022.

[27] "Coppel guideline," https://coppelmx.my.site.com/sellers/s/terminos-y-condiciones-vendedor, 2023, [Online; accessed 15-February-2023].

[28] "How covid-19 changed e-commerce: sales growth and irreversible dependence," https://www.thedrum.com/opinion/2021/01/13/how-covid-19-changed-e-commerce-sales-growth-and-irreversible-dependence, 2021, [Online; accessed 17-February-2023].

[29] "Daraz guideline," https://university.daraz.pk/course/learn?id=937&type=policies&login=skip#drop, 2023, [Online; accessed 15-February-2023].

[30] Z. Y. Dennis, T. Cheong, and D. Sun, "Impact of supply chain power and drop-shipping on a manufacturer's optimal distribution channel strategy," *European Journal of Operational Research*, 2017.

[31] "Drop-shipping: What you need to know before you buy or sell online," https://www.michigan.gov/ag/consumer-protection/consumer-alerts/consumer-alerts/shopping/before-you-buy-or-sell-online, 2022, [Online; accessed 15-February-2023].

[32] "Coronavirus pandemic adds $219 billion to us ecommerce sales in 2020-2021," https://www.digitalcommerce360.com/article/coronavirus-impact-online-retail/, 2021, [Online; accessed 17-February-2023].

[33] "E-commerce jumped 55% during covid to hit $1.7 trillion," https://www.forbes.com/sites/johnkoetsier/2022/03/15/pandemic-digital-spend-17-trillion/?sh=c74ad2350352, 2021, [Online; accessed 17-February-2023].

[34] "ebay guideline," https://www.ebay.com/help/selling/posting-items/setting-postage-options/drop-shipping?id=4176, 2023, [Online; accessed 15-February-2023].

[35] "ebay frowns on orders wrapped in amazon smiles," https://www.ecommercebytes.com/2019/01/21/ebay-frowns-on-orders-wrapped-in-amazon-smiles/, 2021, [Online; accessed 17-January-2023].

[36] "Drop shipping and product sourcing," https://www.ebay.com/help/selling/posting-items/setting-postage-options/drop-shipping?id=4176, 2020, [Online; accessed 11-March-2023].

[37] "Report an issue with a seller," https://www.ebay.com/help/buying/working-sellers/report-seller-listing?id=4022, 2021, [Online; accessed 17-March-2023].

[38] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Conference on Human Factors in Computing Systems*, 2019.

[39] "Feedbackexpress," https://www.feedbackexpress.com/, 2020, [Online; accessed 11-March-2023].

[40] "Flipkart guideline," https://seller.flipkart.com/sell-online/terms-of-use, 2023, [Online; accessed 15-February-2023].

[41] "forum.alidropship," https://forum.alidropship.com/, 2023, [Online; accessed 13-January-2023].

[42] "forum.donanimhaber," https://forum.donanimhaber.com/, 2023, [Online; accessed 13-January-2023].

[43] J. Franklin, A. Perrig, V. Paxson, and S. Savage, "An inquiry into the nature and causes of the wealth of internet miscreants." in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2007.

[44] X. Gan, S. P. Sethi, and J. Zhou, "Commitment-penalty contracts in drop-shipping supply chains with asymmetric demand information," *European Journal of Operational Research*, 2010.

[45] "Inside the weird, get-rich-quick world of dropshipping," https://www.wired.co.uk/article/dropshipping-instagram-ads, 2022, [Online; accessed 15-February-2023].

[46] "google-search-api," https://pypi.org/project/Google-Search-API/, 2021, [Online; accessed 15-February-2023].

[47] "googletrans 3.0.0," https://pypi.org/project/googletrans/, 2021, [Online; accessed 13-January-2023].

[48] "Grey market," https://www.investopedia.com/terms/g/graymarket.asp, 2020, [Online; accessed 11-February-2023].

[49] S. Hao, K. Borgolte, N. Nikiforakis, G. Stringhini, n. Egele, M. Eubanks, B. Krebs, and G. Vigna, "Drops for stuff: An analysis of reshipping mule scams," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2015.

[50] "Helium 10," https://www.helium10.com/, 2020, [Online; accessed 11-March-2023].

[51] "Hepsiburada guideline," https://akademi.hepsiburada.com/portal, 2023, [Online; accessed 15-February-2023].

[52] V. Hovelaque, L. G. Soler, and S. Hafsa, "Supply chain organization and e-commerce: a model to analyze store-picking, warehouse-picking and drop-shipping," *4OR*, 2007.

[53] "informed.co," https://www.informed.co/, 2020, [Online; accessed 11-March-2023].

[54] "Interview protocol (submission-39)," https://osf.io/sqy7z/, 2022, [Online; accessed 15-February-2023].

[55] "Jumia guideline," https://sellercenter.jumia.com.ng/delivery_guidelines, 2023, [Online; accessed 15-February-2023].

[56] "Jungle scout," https://www.junglescout.com/, 2020, [Online; accessed 11-March-2023].

[57] "kaskus.co.id," https://kaskus.co.id, 2023, [Online; accessed 13-January-2023].

[58] A. Kharraz, W. Robertson, and E. Kirda, "Surveylance: automatically detecting online survey scams," in *IEEE Symposium on Security and Privacy (S&P)*, 2018.

[59] M. Khouja, "The evaluation of drop shipping option for e-commerce retailers," *Computers & Industrial Engineering*, 2001.

[60] "Lazada guideline," https://sellercenter.lazada.com.ph/seller/helpcenter/drop-shipping-policy-13852.html, 2023, [Online; accessed 15-February-2023].

[61] S. Ma, Z. Jemai, E. Sahin, and Y. Dallery, "The news-vendor problem with drop-shipping and resalable returns," *International Journal of Production Research*, 2017.

[62] D. McCoy, H. Dharmdasani, C. Kreibich, G. M. Voelker, and S. Savage, "Priceless: The role of payments in abuse-advertised goods," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2012.

[63] "Mercari guideline," https://www.mercari.com/us/help_center/topics/account/policies/prohibited-conduct/, 2023, [Online; accessed 15-February-2023].

[64] S. Mirza, L. Begum, L. Niu, S. Pardo, A. Abouzied, P. Papotti, and C. Pöpper, "Tactics, threats & targets: Modeling disinformation and its mitigation," in *NDSS*, 2023.

[65] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker, "An analysis of underground forums," in *ACM SIGCOMM conference on Internet measurement conference*, 2011.

[66] "Myantra guideline," https://partners.myntrainfo.com/termsofuse, 2023, [Online; accessed 15-February-2023].

[67] S. Netessine and N. Rudi, "Supply chain structures on the internet: and the role of marketing-operations interaction," *Handbook of quantitative supply chain analysis: Modeling in the e-business era*, 2004.

[68] "Noon guideline," https://help.noon.partners/hc/en-us/articles/13411717180695-Product-Listing-Policy, 2023, [Online; accessed 15-February-2023].

[69] "Noon terms," https://help.noon.partners/hc/en-us/articles/8546655990935-International-Seller-Terms-and-Conditions-in-UAE, 2023, [Online; accessed 15-February-2023].

[70] A. Oest, P. Zhang, B. Wardman, E. Nunes, J. Burgis, A. Zand, K. Thomas, A. Doupé, and G.-J. Ahn, "Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale," in *USENIX Security*, 2020.

[71] "Ozon guideline," https://docs.ozon.ru/global/en/fulfillment/rfbs/logistic-settings/order-packaging-requirements/?country=OTHER, 2023, [Online; accessed 15-February-2023].

[72] "packtrack," http://www.packtrack.com/, 2021, [Online; accessed 15-February-2023].

[73] "Dropshipping business training," https://panel.eticaretegitimkursu.com/, 2022, [Online; accessed 13-January-2023].

[74] "Public document sharing tool," https://www.pastefs.com/, 2020, [Online; accessed 13-January-2023].

[75] S. T. Peinkofer, T. L. Esper, R. J. Smith, and B. D. Williams, "Assessing the impact of drop-shipping fulfilment operations on the upstream supply chain," *International Journal of Production Research*, 2019.

[76] R. S. Portnoff, S. Afroz, G. Durrett, J. K. Kummerfeld, T. Berg-Kirkpatrick, D. McCoy, K. Levchenko, and V. Paxson, "Tools for automated analysis of cybercriminal markets," in *International Conference on World Wide Web*, 2017.

[77] U. Porwal and S. Mukund, "Credit card fraud detection in e-commerce," in *IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom)*, 2019.

[78] M. Rahman, N. Hernandez, R. Recabarren, S. I. Ahmed, and B. Carbunar, "The art and craft of fraudulent app promotion in google play," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019.

[79] "ecommerce fulfillment services | rakuten super logistics," https://www.shipnetwork.com/, 2021, [Online; accessed 13-January-2023].

[80] "Reddit dropshipping," https://www.reddit.com/r/dropship/, 2023, [Online; accessed 13-January-2023].

[81] "Repricerexpress," https://www.repricerexpress.com/, 2020, [Online; accessed 11-March-2023].

[82] B. Saunders, J. Sim, T. Kingstone, S. Baker, J. Waterfield, B. Bartlam, H. Burroughs, and C. Jinks, "Saturation in qualitative research: exploring its conceptualization and operationalization," *Quality & quantity*, 2018.

[83] "Sellerengine," https://sellerengine.com/, 2020, [Online; accessed 11-March-2023].

[84] "Feedback genius," https://www.sellerlabs.com/feedback-genius, 2020, [Online; accessed 11-March-2023].

[85] "Shopeee guideline," https://help.shopee.com.my/portal/article/77215, 2023, [Online; accessed 15-February-2023].

[86] "Shopify guideline," https://help.shopify.com/en/manual/your-account/legal/dropshipping, 2023, [Online; accessed 15-February-2023].

[87] "Dropshipping," https://help.shopify.com/en/manual/products/dropshipping, 2020, [Online; accessed 11-March-2023].

[88] "Thousands of fraudsters are selling via shopify, analysis finds," https://www.ft.com/content/0280592d-0adf-4dcb-a831-4f8a85f414bc, 2021, [Online; accessed 17-January-2023].

[89] "Report an issue with a merchant," https://www.shopify.com/legal/report-aup-violation, 2021, [Online; accessed 17-January-2023].

[90] "This shopify side hustle could make you 50k before the holidays," https://nypost.com/2022/11/03/shopify-side-hustle-could-make-you-50k-before-the-holidays/, 2022, [Online; accessed 15-February-2023].

[91] B. Stone-Gross, R. Abman, R. A. Kemmerer, C. Kruegel, D. G. Steigerwald, and G. Vigna, "The underground economy of fake antivirus software," in *Economics of information security and privacy III*. Springer, 2013.

[92] Z. Sun, A. Oest, P. Zhang, C. Rubio-Medrano, T. Bao, R. Wang, Z. Zhao, Y. Shoshitaishvili, A. Doupé, G.-J. Ahn *et al.*, "Having your cake and eating it: An analysis of concession-abuse-as-a-service," in *USENIX Security*, 2021.

[93] Z. Sun, C. E. Rubio-Medrano, Z. Zhao, T. Bao, A. Doupé, and G.-J. Ahn, "Understanding and predicting private interactions in underground forums," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, 2019.

[94] "Target guideline," https://corporate.target.com/_media/TargetCorp/about/pdf/Target-Drop-Ship-Eligibility.pdf, 2023, [Online; accessed 15-February-2023].

[95] K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. G. Kelley, D. Kumar *et al.*, "Sok: Hate, harassment, and the changing landscape of online abuse," in *IEEE Symposium on Security and Privacy (S&P)*, 2021.

[96] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki *et al.*, "Data breaches, phishing, or malware? understanding the risks of stolen credentials," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2017.

[97] K. Thomas, D. McCoy, C. Grier, A. Kolcz, and V. Paxson, "Trafficking fraudulent accounts: The role of the underground market in twitter spam and abuse," in *USENIX Security*, 2013.

[98] "Tiktok influencer bidding to attract investors to his latest get-rich-scheme," https://www.dailymail.co.uk/news/article-11446625/TikTok-star-bidding-attract-investors-latest-rich-scheme-failed-attempt.html, 2022, [Online; accessed 15-February-2023].

[99] "Free trademark search tool," https://www.trademarkia.com/, 2020, [Online; accessed 13-January-2023].

[100] "Trendyol guideline," https://akademi.trendyol.com/satici-bilgi-merkezi/detay/355, 2023, [Online; accessed 15-February-2023].

[101] R. Van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi, C. H. Ganan, B. Klievink, N. Christin, and M. Van Eeten, "Plug and prey? measuring the commoditization of cybercrime via online anonymous markets," in *USENIX Security*, 2018.

[102] "Viral launch," https://viral-launch.com/, 2020, [Online; accessed 11-March-2023].

[103] "voz.vn," https://voz.vn, 2023, [Online; accessed 13-January-2023].

[104] "Walmart guideline," https://sellerhelp.walmart.com/s/guide?article=000007893, 2023, [Online; accessed 15-February-2023].

[105] P. Wang, X. Liao, Y. Qin, and X. Wang, "Into the deep web: Understanding e-commerce fraud from autonomous chat with cybercriminals," in *NDSS*, 2020.

[106] "dropshipping - warrior forum - the #1 digital marketing forum & marketplace," https://www.warriorforum.com/, 2023, [Online; accessed 13-January-2023].

[107] "Wayfair guideline," https://rise.articulate.com/share/DiNQ8Er1YHH-bcFmo_jo5FmJqP7RKOio#/lessons/FY0p2S_UllofFsd3S8TJOkMF-hrZbGbr, 2023, [Online; accessed 15-February-2023].

[108] D.-Q. Yao, X. Yue, S. K. Mukhopadhyay, and Z. Wang, "Strategic inventory deployment for retail and e-tail stores," *Omega*, 2009.

[109] "Amazon vn," https://www.youtube.com/c/AMAZONVN1525, 2023, [Online; accessed 13-January-2023].

[110] "Dropshipping case studies," https://www.youtube.com/channel/UCqw27ZfS4aWdNhP1MDOldPA, 2023, [Online; accessed 13-January-2023].

[111] K. Yuan, H. Lu, X. Liao, and X. Wang, "Reading thieves' cant: automatically identifying and understanding dark jargons from cybercrime marketplaces," in *USENIX Security*, 2018.

[112] F. Zhao, D. Wu, L. Liang, and A. Dolgui, "Lateral inventory transshipment problem in online-to-offline supply chain," *International Journal of Production Research*, 2016.

[113] Y. Zhu, D. Xi, B. Song, F. Zhuang, S. Chen, X. Gu, and Q. He, "Modeling users' behavior sequences with hierarchical explainable network for cross-domain fraud detection," in *The Web Conference*, 2020.

APPENDIX A
E-COMMERCE PLATFORM GUIDELINES

We analyzed guidelines for 20 popular e-commerce platforms. These popular marketplaces provide services to customers in different regions of the world (Europe, Africa, North and South America, and Asia).

Table V presents relevant excerpts from e-commerce guidelines, which sellers are required to follow per the Terms of Use. Broadly, abusive dropshippers violate platform-stipulated guidelines on (1) agreements/communications with suppliers, (2) shipping and packaging, and (3) stock control requirement (necessity to always verify sufficient stock or to remove their listing otherwise). We note that violations of these guidelines are rooted in the lack of a contract/agreement between abusive dropshippers and their "suppliers" (private sellers).

APPENDIX B
CRAWLER KEYWORDS

Table VI shows the queries used in our `Google` Search API crawler for the initial discovery of abusive dropshipping-related forums and resources, described in Sec. III.

TABLE V: Studied marketplaces and corresponding guidelines that ban abusive dropshipping.

Marketplace	Excerpt of Guideline that prohibits Abusive Dropshipping
eBay	*Listing an item on eBay and then purchasing the item from another retailer or marketplace that ships directly to your customer is not allowed on eBay* [34]
Amazon Canada	*Have an agreement with your supplier that they will identify you (and no one else) as a seller of your products on all packing slips, invoices, external packaging* [10]
Amazon US	*Purchasing products from a third party, including Amazon or another seller in Amazon's stores, and having that third party ship directly to customers ... is strictly prohibited without exception* [12]
Shopeee	*Seller shall properly manage and ensure that relevant information such as the price and the details of items, inventory amount and terms and conditions for sales is updated on Seller's listing and shall not post inaccurate or misleading information* [85]
Lazada	*A seller shall not perform [import] and [list] large volume of existing products listed for sale by another seller* [60].
Flipkart	*You must have all the necessary licenses and permits required for such sale. All listed items must be kept in stock for successful fulfillment of sales* [40]
Target	*Accommodation of all carriers and shipping services... [and] ability to produce a Target.com branded pack slip for every shipment* [94]
Trendyol	*Packaging materials bearing the brands and logos of other e-commerce platforms should not be used, the seller should check the stock, price, and suitability for shipping to the customer, both physically and systematically*‡ [100]
Mercari	*Prohibited conduct: Listing items not in your possession, Listing an item that is not actually for sale* [63]
Walmart	*Marketplace sellers may not purchase products from another retailer and have the order shipped directly to a Walmart customer* [104]
Daraz	*The Seller is obliged to maintain inventory of all Products featured on the Platform and update its true inventory through the Seller Center on a daily basis [29]*
Myantra	*You must be legally able to sell the item(s) you list for sale on our Platform and must have all the necessary licences and permits required for such sale* [66]
Wayfair	*Fulfillment of any product using non-Wayfair or non-supplier packaging... branded packaging from other retailers. is strictly prohibited* [107]
Shopify	*Before using the dropshipping fulfillment method, make sure that you choose a reputable supplier - Read the supplier's policies and Talk with the supplier about their business* [86]
Coppel	*The Parties agree that the delivery of the Products to the Client will be carried out using the shipping packages that Coppel provides through the platform*‡ [27]
Hepsiburada	*The seller shall not use any packaging/package belonging to another platform during the packaging processes*‡ [51]
AliExpress	*The Seller represents that it is and undertakes to be, during the term of the Agreement, the holder of all the rights over the published products* [3]
Ozon	*When shipping your parcels, print the label from your Ozon personal account and stick it on the package* [71]
Jumia	*Use the buyer payment receipt and put it inside the package, only Jumia shipping labels may be used* [55]
Noon	*Obtain all necessary documentation, permits and consents to deliver the product, only QR codes provided by noon, or which you can print from Seller Lab should be properly applied on each package* [68], [69]

‡ Translated to English via Google Translate.

TABLE VI: Queries used in data collection crawling process.

Queries Used For Crawling‡	
`dropshipping fraud`	`dropshipping evasion`
`dropshipping easy setup`	`dropshipping from amazon`
`dropshipping copyright`	`dropshipping avoid flag`
`dropshipping configuration`	`dropshipping easy business`
`dropshipping fulfillment`	`dropshipping suppliers`
`dropshipping markup`	`dropshipping from aliexpress`
`dropshipping taxes`	`dropshipping products`
`dropshipping guide`	`dropshipping no agreement`
`dropshipping avoid fees`	`dropshipping ebay shopify`
`dropshipping without permission`	`dropshipping shipping label`
`dropshipping find suppliers`	`dropshipping suppliers report`
`dropshipping seller finding out`	`dropshipping legal issues`

‡ Crawling was repeated by replacing instances of the word "dropshipping" with the alternate spelling "drop shipping."

APPENDIX C
CODEBOOKS FROM THEMATIC ANALYSIS

We present three codebooks generated from our analysis. We note prevalence through our predefined qualitative terminology (**f**, **s**, **m**, **a**), for low-level themes.

Key: ◇ High-level code, ○ Low-level code

A. Forum Threads

We present our codebook generated during our analysis of forum threads (**F**).

◇ **Abusive item sourcing**
○ opting for items exclusive to target domain (**a**)
○ offering lower priced alternatives (competitive profit) (**a**)
○ avoiding trademarked items (**a**)

◇ **Underground collaboration to source items**
○ identifying "non-risky" brands (**s**)
○ identifying gap items proven to be successful (**s**)
○ forging documents (**f**)

◇ **Leveraging software**
○ abusive use of benign software (**a**)
○ using software marketed for malicious use (**m**)

◇ **Volatile item fulfillment**
○ not providing shipping information (**s**)
○ generating fake tracking numbers (**f**)
○ delayed or neglected orders (**s**)

◇ **Complications in return process**
○ refund due to inconvenience in shipping returns (**f**)

◇ **Abusive dropshipping characteristics**
○ diversity of item categories (**a**)
○ avoiding reliance on one brand (**s**)
○ preferring non-trademarked items (**a**)
○ geographic location that is different from target market (**s**)
○ preference of lower priced items (**s**)

B. Instructional Material

We present our codebook generated during our analysis of instructional material (**M**).

◇ **Abusive item sourcing**
○ opting for exclusive items (**a**)
○ pricing items competitively (**a**)
○ avoiding trademarks/known brands (**a**)
○ forged documents (**f**)

◇ **Leveraging software**
○ abusive use of benign software (**a**)

◇ **Use of malicious software**
○ trademark filtering (**m**)

◇ **Dropshipping characteristics**
○ avoiding expensive items (**s**)
○ preferring non-trademarked items (**s**)
○ targeting different countries (**s**)

C. Interviews

We present our codebook generated after we analyzed interview transcripts (**I**).

◇ **Pricing intricacies affecting sellers**
○ price hike (**a**)
○ quality-price mismatch (**m**)

◇ **Impact on seller reputation**
○ negative reviews (**m**)
○ reputation loss (**m**)
○ low ratings (**m**)
.

◇ **Abusive dropshipper preferences/characteristics**
○ exclusive items (**s**)
○ competitive profit items (**s**)
○ avoiding trademarked items (**a**)

◇ **Abusive dropshipper malicious actions**
○ forged documents (**s**)
○ generating fake tracking numbers (**f**)

◇ **Abusive dropshipping impact on customers**
○ return complications (**m**)
○ withholding shipment information (**m**)
○ neglected/delayed orders (**m**)