Analyzing Supply and Demand Signals for Cybercrime Services in Technical-Support Scams

Raghavendra Cherupalli
School of Cyber Studies
The University of Tulsa
Tulsa, USA
rac8609@utulsa.edu

Yi Ting Chua
School of Cyber Studies
The University of Tulsa
Tulsa, USA
ytc2805@utulsa.edu

Tyler Moore
School of Cyber Studies
The University of Tulsa
Tulsa, USA
tyler-moore@utulsa.edu

Gary Warner
Director of Intelligence
Dark Tower
Birmingham, USA
gary.warner@getdarktower.com

***Abstract*—Like many cybercrimes, technical-support scam (TSS) is comprised of a series of operational phases. Personal data for outreach must be obtained first. Potential victims are then targeted by a variety of baiting techniques, after which fraudulent communication is initiated. The scam ends in financial extraction and laundering of the criminal proceeds. Each step of the process may be provided by one or more criminal actors. We empirically investigate the supply and demand for such services in the TSS ecosystem by examining dedicated Facebook groups operated by cybercriminals. We develop a system to automatically categorize 312,586 posts, identifying the service and whether the post advertised or requested the service. The automated classification process adopts an AI-based methodology in which a pre-trained Natural Language Inference (NLI) model is fine-tuned using human-labeled data. We evaluate the results to understand the key players' roles, their behavior of advertising (supplying) and requesting (demanding) across the service categories. We also examine the structural and operational dynamics of the fraudulent ecosystem. The results could provide actionable intelligence for law enforcement and policymakers by differentiating the structural roles, market segmentation and cross-category relationships to help establish key strategic intervention points.**

***Index Terms*—tech support scams, cybercrime measurement, natural language inference, cyber criminology**

I. Introduction

In a technical-support scam (TSS), sometimes known as a call-center or impersonation scam, a criminal impersonates a legitimate service provider by offering "assistance" designed to defraud victims [1]. In the United States, the FBI's 2025 Internet Crime Complaint Center (IC3) has highlighted the growing magnitude of the TSS threat, recording more than 80,000 complaints with total losses surpassing USD$2.9 billion [2]. Compared to 2024, complaints increased by 122% and losses rose by 98% [3]. TSS is a persistent and evolving form of online fraud that preys upon users seeking assistance for real or perceived technical issues. Traditionally associated with aggressive browser-locking tactics and phone-based impersonation [4], [5], modern TSS operations have expanded their reach, complexity, and scale. The Federal Trade Commissions (FTC) noted the use of fake invoices and subscription renewals by scammers to lure users into calling [6].

Recent studies demonstrated the transformation of TSS to highly organized operations involving dedicated websites, toll-free numbers vendors, call centers, underground markets, and money laundering services [7], [8]. The ecosystem is sustained through public social media platforms such as Facebook, Telegram and WhatsApp, which are used to advertise services, hire agents, and disseminate scam-related infrastructure. These studies demonstrate that TSSs rely on a marketplace of vendors, platforms, intermediaries, and service models rather than isolated actors.

Shutting down individual scams, while important, is not efficient, as criminals can establish new scams more quickly than it takes to extinguish old ones. It is therefore necessary to examine the ecosystem that supports large-scale scam operations. By leveraging a large corpus of public communications among TSS actors in Facebook groups, the study offers insights and perspectives on the supply-and-demand dynamics within the marketplaces. The study is structured around the following key research questions:

RQ1: What services are supplied together more and less frequently?
RQ2: What services are demanded together more and less frequently?
RQ3: What services are supplied and demanded together?
RQ4: To what extent do supply and demand behaviors evolve over time among top actors?

A. Key Contributions

This paper offers important empirical insights and methodological contributions to the study of TSS marketplaces:

- *Specialization of Actors:* We investigate the key actors' concentration on specific service categories. The specialization is maintained on both both supply and demand sides, and a tiny minority of 0.33% users dominates the market by contributing one-third of the total volume.
- *Structural Patterns and Operational Clustering:* We examine cross-posting behavior of top users to understand the organizational structure and functional pairing of certain services. The evidence shows that related services exhibit systematic cross-posting, such as across victim data-blasting campaigns and toll-free number providers, or by job offerings and web development services. This demonstrates the complementary capabilities necessary for successful execution of the scam.

- *Natural Language Inference (NLI) Model for Post-Type Classification:* We fine-tune and test the applicability of an NLI model classifier to categorize the cyber-criminal posts based on underlying motivation. Unlike typical NLI tasks and datasets, this task presents additional challenges due to the frequent use of ungrammatical and underground community jargon. The results indicate a significant accuracy after small-sample fine-tuning.

II. Related Work

A. Tech Support Scams

The tactical transition of TSS was first systematically documented by Miramirkhani et al. [9] who identified malvertising as a primary vector of the scam operations. Srinivasan et al. [5] subsequently expanded this understanding by investigating web domain infrastructure supporting the TSS, explaining how the criminals use black hat search engine optimization techniques for redirecting victims to fraudulent websites. This research established the basic importance of understanding TSS not as a isolated lone criminal act but as a complex, interdependent criminal ecosystem.

Rauti et al. [4] conducted an innovative empirical investigation by interacting with 10 active tech support scammers to document the TSS operational methodologies. The observations revealed a consistent pattern: (1) victims initially encountered fake websites, (2) scammers initiated communication through live chat or cold calling techniques, (3) victims are subsequently directed to install remote access software, (4) after initializing the remote session scams, scammers misuse legitimate system tools to perform unnecessary clean-ups, and (5) victims are directed to make a payment where scammers maintained their remote connection during the payment processing. In addition, the study explored the variation in payment methods preferred by different actors. Larson et al. [10] approached the TSS problem technically by developing an artificial intelligence (AI) driven pipeline to detect TSS websites. Both studies further provide concrete evidence of multi-component architecture of TSS ecosystems integrating multiple specialized services.

Detailed investigation of infrastructure supporting the TSS required analyses beyond the victim counterfeit websites and operational tactics. Liu et al. [8] provided crucial findings about the TSS ecosystem by examining real-time communications within Facebook and WhatsApp groups that are explicitly created for assisting scammers. The study provided direct evidence of criminals using mainstream platforms for coordination, along with underground forums. Cherupalli et al. [7] extended this foundation via detailed examination of such Facebook groups which are not only acting as a communication channel but also as an informal marketplace where scam operators could exchange various components or services needed to operate the TSS ecosystem. To develop an automated classification, Cherupalli et al. [7] employed structured LLM prompting with few-shot in-context-learning technique, where Gemma3:12B model was provided with small number of examples to guide the classification process accurately.

B. Specialization in Online Criminal Market Places

Research on online criminal marketplaces has since examined specialization both at the vendor and market levels. At the market-level, specialization is broader and organized around types of cybercriminal activities. For example, markets such as SilkRoad and Alphabay specialize in prescription drugs and illegal substances [11]–[13]. For cybercriminals interested in online stolen data, there were marketplaces such as ShadowCrew [14] and Crimenetwork [15]. These marketplaces not only specializes in products (e.g., fullz which are data that contains the complete information needed for using stolen card or bank account, including birth dates, mother's maiden name, etc.), but also provide products that are useful for obtaining or using the data [15], [16]. For TSS, there are also specialized marketplaces for products and services necessary for operations [8].

At the vendor-level, specialization tends to occur within product and service categories, where vendors focus their offerings within a specific category. The motivation for such specialization is to establish credibility and competitive advantages [11], [13]. Based on characteristics such as experience and reputation, van Wegberg et al [13] conducted clustering analysis to examine whether there are distinct patterns among sellers on AlphaBay. Using latent profile analysis, they identified five vendor profiles that significantly influence sales performance: (1) freelancer, (2) generalist, (3) specialist, (4) professional, and (5) loafer. With the exception of the loafer profiles, all vendor profiles increased in lifespan and successes. The loafer profile had the lowest level of exposure and experience and generated very little revenue compared to all other vendor profiles. The study also showed that vendor characteristics strongly influence product sales outcomes, where vendor and product attributes explained up to 47% of the variance in product sales. In this case, specialization is seen as a potential signal of expertise and reliability.

However, specialization is not universal. While examining multiple carding forums, Haslebacher et al [15] found that across five forums, only 38.1% of all users focused on selling one type of product. The authors did observe variations: some users exhibit within-category specialization by offering multiple variants of a single product type (e.g., credit cards from different geographic regions), whereas others demonstrate cross-category diversification, providing products across multiple categories with limited variation within each category [15]. One possible factor for such variations in vendor-level specialization is the barrier of entry. Holt and Lee [17] found that specialization tends to concentrate within products such as malware or counterfeit identity documents due to the knowledge and tooling required. These findings highlight that vendor-level specialization is affected by market structures and technical complexity of products/services.

C. Natural Language Inference

Existing research on identifying the intention from the text has traditionally relied on two techniques: topic modeling [18] and keyword based heuristics [19]. Topic modeling is a statistical method of clustering related words that appear together, exposing common topics and subjects discussed in the statements. Keyword based heuristics primarily flag the post depending on certain keywords provided. Both of these methods often provide very useful foundational information, but lack the capacity to detect the motivation in the text. Sentiment analysis is a natural language processing approach that is mainly useful for detecting whether the text is towards a positive tone or a negative tone [20]. In the dataset utilized for this study, there are many instances such as "anyone need the e-mail blasting data Ping me" , "I need e-mail blasting data Dm me". Both of the above sentences are speaking about data which would be grouped together by topic modeling and keyword based heuristics. Also, both the sentences attained a positive tone. In reality, the two sentences fundamentally are on different sides in the marketplace where the first sentence was offering the service, and the later sentence was requesting the service.

Natural language inference (NLI) solves this problem using a more robust framework by evaluating the logical relationship between a premise and a hypothesis rather than matching keywords or clustering topics [21]. The fundamental principle of NLI is deciding whether a premise entails hypothesis, contradicts, or is neutral. This enables a more polished interpretation of motivation in the text. Modern NLI models are developed on transformer-based models, particularly bidirectional encoder representations from Transformers (BERT) [22], RoBERTa (a robustly optimized version of BERT) [23], and DeBERTa (Decoding enhanced BERT with disentangled attention) [24]. The transformer-based pre-trained models hold the key advantage of transfer learning. Research in this domain has proved the models can achieve greater accuracy and performance when they are fine-tuned with tens and hundreds of task specific examples [25], [26]. In recent years, Laurer et al. [27] developed a universal classifier which was trained on 33 datasets and 389 variety of class categories. In his study Laurer et al. [27] explained fine tuning the developed model with few number of examples can yield much greater results than zero-shot classifier.

III. Methodology

The current study examines the dynamics within the TSS marketplaces on Facebook. More specifically, we are focusing on transactional post content, as well as selling and buying behaviors among active actors across time. To do so, we utilize a comprehensive dataset introduced in [7], which consists of 96 Facebook groups that were explicitly created to assist TSS or demonstrated tolerance for the trading of illicit services supportive of TSS operations. There are a total of 186,936 users in total. Within this network, 381,843 posts were posted across these groups from the time period of April 2015 to March 2024.

TABLE I
Descriptions of Product/Service Categories

Category	Definition
Money-Laundering Services (MLS)	Services that cash out or transfer stolen payments
Fake/Illicit Document Services (FDS)	Impersonating the documents of legitimate organizations, as well as fake IDs.
Victim Data Sales (VDS)	Data of victim contact or personal details.
Blasing Campaign Services (BCS)	Services that transmit mass email or SMS messages to prospective victims using the technique called email/SMS blasting, by which inbound calls are generated.
PPC/Popup Calls (PPC)	Services that assist scammers in running malware advertising campaigns, such as PPC and pop-ups to generate inbound calls.
Job Offerings (JO)	Hiring workers that take phone calls at call centers.
Criminal IT Infrastructure Operations (CIO)	Scripts and tools required to operate criminal IT infrastructure, excluding toll free number providers, website development services and remote access services.
Toll-Free Number Providers (TNP)	Toll-free number (TFN) numbers used to contact victim.
Remote Access Services (RAS)	Remote access software used to connect to victim devices.
Web Development Services (WDS)	Website services, including hosting and promotion.

A. Product/Service Categorization

In total, 312,586 out of 381,843 posts were categorized into 12 core components that support TSS operations consisting of (1) Money Laundering Services, (2) Fake/Illicit Document Services, (3) Victim Data Sales, (4) Blasting Campaign Services, (5) PPC/Popups Calls, (6) Job Offerings, (7) Criminal IT Infrastructure Operations, (8) Toll-Free Number Providers, (9) Remote Access Services, (10) Web Development Services, (11) Scammer Warnings, and (12) Others. Table I provides definitions for each category.

The classification scheme is adopted from [7] and was a result of iterative ground truth labeling. The remaining 69,257 posts were excluded due to non-English text language or failure in label generation.

B. Manual Categorization of Supply-and-Demand Signals

1) Training Data Annotation: A random sample of 1,000 posts was selected and manually labeled by a human annotator, following the process adapted from modified grounded theory. Each post was assigned to one of the three distinct post-type categories based on the predominant intention of each post. The classification scheme consists of the following

- *Advertisement* posts, which offer services or products that can facilitate the TSS operations.
- *Request* posts, which seek services or products that can streamline the TSS scams.
- *General* posts, encompassing all other post types including discussions, tutorials on criminal scam techniques and

warnings about rippers and law enforcement actors in these groups.

2) Validation Data Annotation: To systematically conduct a rigorous evaluation of the fine-tuned model, a separate validation dataset was created by sampling 100 random posts from the original dataset. The initial review of the validation dataset resulted in 80 valid posts for further analysis, where the remaining posts were either null or posted in non-english language and were excluded. The filtered validation set was independently labeled by two human annotators to ensure reliable ground truth using the same tripartite classification scheme used in the training dataset annotation. Statistical analysis of the annotator agreement is measured using Cohen's Kappa [28], which resulted in 0.924. According to study of Corbin et al. [29], kappa statistic ranging between 0.81 and 1.0 is considered as an *almost perfect* strength of agreement. This metric evaluation explains lucidity in the classification scheme and the resulted validation could be utilized as the ground truth labels for measuring the performance of automation classification.

C. Automation Categorization of Supply-and-Demand Signals

1) Model Training: Fine-tuning the model on an imbalanced dataset can lead the models to bias towards the majority class instead of learning robust category differentiation [30]. To overcome this problem, a balanced sub-dataset of 162 posts was created by selecting an equal number of posts from each category from the 1000 manual labeled data set, resulting in 54 advertisement posts, 54 request posts and 54 general posts [31], [32]. Ensuring class parity, this balanced sub-dataset is then utilized to fine-tune the pre-trained NLI model named *Deberta-v3-large-zeroshot-v1.1-all-33* [27]. The sub-dataset was divided into training and testing subsets using the 80-20 split ratio. The Pre-trained tokenizer from model architecture was utilized for model initialization. The training process was integrated with the model check-pointing and saving techniques at each epoch level, with all intermediate outputs and logs stored.

2) Initial Model Evaluation: After training for eight epochs, the fine-tuned model resulted in an evaluation accuracy of 78.78% in the test set generated from the balanced data set. This performance explains that the model has successfully learned to categorize the posts based on the intent of selling/requesting a service/product or generally discussing about the operations of TSS.

3) Testing Under Realistic Conditions : To assess model's capacity to classify beyond the balanced dataset and perform efficiently on real-world data under realistic conditions, we applied the fine-tuned classifier model on the validation dataset with the annotator's ground truth labels. The model correctly predicted 72 posts out of 80, achieving an overall an accuracy of 90%, particularly higher than the 78.78% accuracy in balanced test set. The improved results explain the classifier's effective generalization to unseen data. The weighted F1-score of 0.91 indicates robust performance considering the natural distribution of the categories. Detailed evaluation metrics are provided in the Appendix A.

D. Analysis

The fine-tuned NLI model was applied to the dataset of 312,586 product/service categorized posts to label them according to the intention expressed in the text into three categories. To better understand how these marketplaces operate, the researchers identified the top 100 users who were active and posted for at least three years. The temporal criterion helps us identify users who maintain active presence with committed and sustained investment in the marketplaces. This group of users collectively accounted for one-third of the total posts (n = 97,681). This indicates that a small percentage of powerful users play a central role in dictating the transactional dynamics of the marketplaces.

Prior to the co-posting analysis, the researchers established an initial clustering that organized the ten service/product categories based on their functional roles within TSS execution. The clustering identified five functional groups: (1) *Cashout*, comprising of *Money Laundering Services* and *Fake/Illicit Document Services*, representing the monetization and identity infrastructure for finacial extraction; (2) *Data* consisting *Victim Data Sales* as a standalone category, given it's foundational position as primary input; (3) *Luring*, encompassing *Blasting Campaign Services* and *PPC/Popups Calls* , which together covers services and tools for victim engagement approaches; (4) *People*, having solely of *Job Offerings*, reflecting human resource placement in TSS operations; (5) *Technical Infrastructure*, which integrates *Toll-Free Number Providers*, *Criminal IT Infrastructure Operations*, *Remote Access Services*, and *Web Development Services*, as back-end technical capabilities and infrastructures necessary for scam execution. This framework helps us observe co-posting patterns by situating each service within their broader operational contexts and anticipated complementary relationships.

IV. Results

The results revealed a striking imbalance in the post type distribution. The vast majority of posts (66.22%) offered products/services, followed by 19.74% of posts that were requesting services. The remaining 14.04% of posts were general discussions on techniques and information sharing. The distribution highlights an imbalance in the supply-and-demand ratios in the marketplaces, indicating a vendor-dominated structure. The actors who are suppliers are actively promoting their services irrespective of demands. The distribution of advertisements is approximately three times the distribution of requests, indicating that these groups serve as a marketplace reflecting a mature criminal service economy with organized supply side operations.

To determine the posting behaviors of the actors, we conducted analysis of co-posting matrices that capture advertisement, request, and mixed advertisement-request activities. The matrices provide insight into systematic characterization of market roles and cross-category involvement within the illicit

marketplaces. The categories of *Scammer Warnings* and *Others* were excluded from analysis as these categories typically include content on general and non-transactional discussions. Table II maps to the co-posting matrix of advertisements among the top 100 users by showing the column-normalized percentage of each category (column) authored by users who are active in both the categories (row, column). Table III follows the same structure, presenting the requests of co-posting matrix across the ten product categories. Statistical significance is based on standardized residual analysis. The bold values indicate statistically significant over-representation (residual $> +4, > 99\%$ confidence) and italic values indicates significant under-representation (residual $< -4, > 99\%$ confidence).

A. Supplier Behavior

The percentages of average postings row-wise in Table II provide details on the prominent product and service categories advertised by the top 100 actors. Advertisements on *Victim Data Sales* dominate the marketplace, with the highest mean of 26%, followed by *Money Laundering Services* (18.8%), *Blasting Campaign Services* (18.3%), and *PPC/Popup Calls* (15.4%). All four categories are essential for TSS scam operations regardless of types of tactics. Conversely, *Remote Access Services* (0.4%), *Fake/Illicit Document Services* (0.3%), and *Web Development Services* (0.4%) were among the least advertised products and services by the top 100 actors.

The most significant pattern from Table II appears in the diagonal entries of the matrix, revealing category specialization across all products. Specifically, it highlights that most users who are advertisement-oriented focus on developing expertise rather than diversifying across multiple product and service categories. This is true for six of the ten product and service categories, including *Money Laundering Services*, *PPC/Popup Calls*, and *Victim Data Sales*. *Money Laundering Services* had the largest residual (+175). In addition, users advertising in *Money Laundering Services* were also less likely to post in other product and service categories such as *Toll-Free Number Providers* (7.4%, residual = -59.66). This suggests a systematic disinterest in other categories, elucidating the niche market positioning of *Money Laundering Services*.

Besides specialization, we also observed strong cross-posting patterns concentrated in different domains. First, there are significant co-occurrence between product/service categories that are victim-facing. For example, users who advertised in *Victim Data Sales* also advertised in *Blasting Campaign Services*, accounting for 30.6% of the posts in *Blasting Campaign Services* (overall percentage for *Victim Data Sales* posts is 26.0%). Other co-occurrences include: (1) *PPC/Popup Calls* and *Job Offerings* (29.6%, with overall percentage for *PPC/Popup Calls* being 17.8%), (2) *Blasting Campaign Services* and *PPC/Popup Calls* (23.2%, with overall percentage for *Blasting Campaign Services* being 18.3%), and (3) *Blasting Campaign Services* and *Toll-Free Number Providers* (23.0%, with overall percentage for *PPC/Popup Calls* being 18.3%). These groupings indicate a concentration in supply between victim data and lures, reflecting the complementary nature of operational pipeline in TSS.

Second, there is co-occurrence among technical infrastructure services. Actors active in *Criminal IT Infrastructure Operations* posted more significantly in *Web Development Services* (23.1%) and *Remote Access Services* (15.9%), with the overall percentage of posts for *Criminal IT Infrastructure Operations* being only 6.4%. Similarly, actors in *Toll-Free Number Providers* engage in cross-posting to *Remote Access Services* (20.5%, overall percentage of *Toll-Free Number Providers* = 9.8%). These relations explain the significant clustering that offers the technical infrastructure that is critical during the execution of large-scale fraud operations.

Lastly, we see co-occurrence among cashout services, specifically *Money Laundering Services* and *Fake/Illicit Document Services*. Specifically, we see that actors in *Money Laundering Services* accounted for 34.6% of the posts in *Fake/Illicit Document Services*.

B. Demand Behavior

The co-posting matrix of advertisements explained what vendors offer, while the request co-posting matrix (Table III) provides an overview of what products and services are sought after and required by TSS operations. The row-wise average highlights the importance of different product and service categories as demand drivers. *Blasting Campaign Services* had the highest average cross-category posting (32.6%), suggesting it as a universal infrastructure rather than a specialized product. The next three highest average cross-category posting were substantially lower: *Victim Data Sales* (15.9%), *PPC/Popups Calls* (15.9%), and *Money Laundering Services* (11.6%). On the other hand, products and services such as *Web Development Services* (0.1%), *Toll-Free Number Providers* (1.3%), and *Fake/Illicit Document Services* (2.7%) were not highly demanded by the top 100 actors.

Similarly to the supplier behaviors, we see a strong concentration in the Request matrix (Table III), as indicated by the diagonal values. For example, actors who only requested for *Fake/Illicit Document Services* accounted for 42.3% (residual = +57.8) of posts in that category while the average contribution of the category is only 2.7%. Similar patterns are seen across all product and service categories.

Another pattern we observed is the cross-category posting between *Money Laundering Services* and *Fake/Illicit Document Services*. Specifically, actors who requested for *Money Laundering Services* accounted for 48.0% of all requests for *Fake/Illicit Document Services* (residual = +26.83). The pattern is consistent when flipping the product category. This clustering suggests a tightly coupled demand association between the two categories, which is consistent with the operation of fraud and money laundering [33]. In other words, actors seeking to transfer funds from TSS require documentation infrastructure to acquire or legitimize the funds.

We also see another concentration in cross-posting of requests between *Job Offerings* and *Web Development Services*.

TABLE II
CO-POSTING BEHAVIOR MATRIX FOR ADVERTISEMENT POSTS ACROSS THE PRODUCT/SERVICE CATEGORIES AMONG TOP 100 AUTHOR POSTINGS (COLUMN-NORMALIZED PERCENTAGES AND STATISTICALLY SIGNIFICANT UNDER-REPRESENTATIONS ARE INDICATED IN ITALIC AND OVER-REPRESENTATIONS ARE INDICATED IN BOLD)

	Post Type: Advertisements (Row) – Advertisements (Column)										
	Cashout		*Data*	*Luring*		*People*	*Technical Infrastructure*				
	MLS	**FDS**	**VDS**	**BCS**	**PPC**	**JO**	**CIO**	**TNP**	**RAS**	**WDS**	**Overall**
Money Laundering Services (**MLS**)	**49.3**	**34.6**	*17.9*	*16.6*	*5.4*	*2.0*	**19.9**	*7.4*	*0.5*	*0.4*	18.8
Fake/Illicit Document Services (**FDS**)	**0.5**	**4.8**	0.3	*0.1*	*0.1*	*0.0*	0.4	**0.6**	0.2	0.0	0.3
Victim Data Sales (**VDS**)	*14.6*	*23.3*	**36.9**	**30.6**	*16*	**32.9**	*23.8*	*24.7*	*22.8*	*17.9*	26.0
Blasting Campaign Services (**BCS**)	*11.1*	*7.3*	*16.9*	**19.0**	**23.2**	*12.1*	**20.3**	**23.0**	**22.6**	**21.2**	18.3
PPC/Popups Calls (**PPC**)	*11.6*	*14.3*	*13.7*	18.1	**33.2**	**29.6**	*16.3*	18.5	*12.9*	*13.8*	17.8
Job Offerings (**JO**)	**1.6**	*0.0*	*1.1*	*1.0*	1.9	**8.6**	*0.1*	1.8	*0.1*	*0.1*	1.3
Criminal IT Infrastructure Operations (**CIO**)	*4.3*	*4.0*	*5.3*	*5.5*	**7.0**	6.1	**8.9**	6.1	**15.9**	**23.1**	6.4
Toll-Free Number Providers (**TNP**)	*6.4*	11.1	*7.3*	*8.5*	**12.1**	*8.4*	9.4	**16.8**	**20.5**	**15.2**	9.8
Remote Access Services (**RAS**)	0.4	0.7	*0.3*	*0.3*	0.5	*0.0*	0.5	0.4	**3.1**	**0.9**	0.4
Web Development Services (**WDS**)	*0.2*	*0.0*	*0.4*	*0.4*	0.5	*0.2*	*0.4*	**0.7**	**1.3**	**7.4**	0.4

TABLE III
CO-POSTING BEHAVIOR MATRIX FOR REQUEST POSTS ACROSS THE PRODUCT/SERVICE CATEGORIES AMONG TOP 100 AUTHOR POSTINGS (COLUMN-NORMALIZED PERCENTAGES AND STATISTICALLY SIGNIFICANT UNDER-REPRESENTATIONS ARE INDICATED IN ITALIC AND OVER-REPRESENTATIONS ARE INDICATED IN BOLD)

	Post Type: Requests (Row) – Requests (Column)										
	Cashout		*Data*	*Luring*		*People*	*Technical Infrastructure*				
	MLS	**FDS**	**VDS**	**BCS**	**PPC**	**JO**	**CIO**	**TNP**	**RAS**	**WDS**	**Overall**
Money Laundering Services (**MLS**)	**22.2**	**48.0**	11.0	*8.6*	*8.6*	**14.4**	*8.2*	*5.3*	*7.4*	*0.0*	11.6
Fake/Illicit Document Services (**FDS**)	**7.6**	**42.3**	**4.2**	*0.1*	*0.1*	*0.2*	*0.0*	*0.0*	*0.0*	0.0	2.7
Victim Data Sales (**VDS**)	*9.2*	*6.8*	**30.8**	15.6	*12.7*	*8.5*	*9.8*	**20.4**	*11.5*	*0.0*	15.9
Blasting Campaign Services (**BCS**)	34.7	*0.4*	*25.8*	**36.6**	35.0	35.3	30.6	33.1	**48.1**	*14.9*	32.6
PPC/Popups Calls (**PPC**)	*12.6*	*1.8*	14.7	17.6	**25.1**	*6.3*	14.0	**28.8**	14.1	*0.0*	15.9
Job Offerings (**JO**)	7.2	*0.7*	*4.8*	9.4	6.6	**18.1**	9.5	*2.1*	*4.4*	**77**	8.0
Criminal IT Infrastructure Operations (**CIO**)	5.5	*0.0*	*3.6*	*5.0*	*5.0*	7.4	**20.8**	*3.8*	*1.5*	2.7	6.7
Toll-Free Number Providers (**TNP**)	0.7	0.0	1.2	1.6	1.6	*0.1*	1.1	**5.7**	1.0	0.0	1.3
Remote Access Services (**RAS**)	*0.4*	*0.0*	*3.8*	5.2	5.3	**9.3**	5.7	*0.9*	**12.0**	0.0	4.8
Web Development Services (**WDS**)	0.0	0.0	0.0	0.2	0.0	0.4	0.2	0.0	0.0	**5.4**	0.1

Actors who requested for both *Job Offerings* and *Web Development Services* accounted for 77.0% of all requests made for *Web Development Services*. This suggests that the top 100 actors are recruiting manpower while also procuring technical infrastructure, which would be necessary for TSS operations. We see other cross-posting that highlights various aspects of the TSS operations. For example, there are strong cross-posting behaviors between: (1) *Blasting Campaign Services* and *Remote Access Services* (48.1%), and (2) *PPC/Popup Calls* and *Toll-Free Number Providers* (28.8%). Overall, these pairings highlight a stronger demand for technical infrastructures within these marketplaces.

Apart from cross-posting behavior, the table also highlights patterns of market segmentation when it comes to actors' demand. One prominent example is seen within *Fake/Illicit Document Services* requests. For example, actors requesting for *Fake/Illicit Document Services* are substantially under-represented in requests for *Blasting Campaign Services* (0.1%), and vice versa. This segmentation suggests possible division of labor within TSS operations, especially between victim-facing operations and cashout services.

C. Dual Market Roles

Table IV presents the advertisement-request cross-posting matrix. This 10×20 matrix maps each row category (representing actors' primary activity focus) against paired advertisement and request columns for all ten categories, with cell values representing column-normalized percentages. Statistical significance follows established thresholds: bold values denote over-representation (standardized $residual >$+4), while italicized values indicate under-representation ($residual < -4$). This matrix demonstrates whether actors advertising in one service simultaneously seek or sell another service,

TABLE IV
CROSS-CATEGORY ADVERTISEMENT AND REQUEST CO-POSTING MATRIX ACROSS THE PRODUCT/SERVICE CATEGORIES AMONG TOP 100 AUTHOR POSTINGS (COLUMN-NORMALIZED PERCENTAGES AND STATISTICALLY SIGNIFICANT UNDER-REPRESENTATIONS ARE INDICATED IN ITALIC AND OVER-REPRESENTATIONS ARE INDICATED IN BOLD)

	Cashout				*Data*		*Luring*				*People*		*Technical Infrastructure*								**Overall**
	MLS		**FDS**		**VDS**		**BCS**		**PPC**		**JO**		**CIO**		**TNP**		**RAS**		**WDS**		
	Adv	**Req**	**Adv**	**Req**	**Adv**	**Req**	**Adv**	**Req**	**Adv**	**Req**	**Adv**	**Req**	**Adv**	**Req**	**Adv**	**Req**	**Adv**	**Req**	**Adv**	**Req**	
MLS	**39.6**	**13.3**	**21.4**	*1.4*	*3.5*	*5.3*	*6.4*	12.2	11.3	**14.0**	**27.5**	**15.9**	*6.8*	**30.6**	*3.5*	11.1	*0.9*	4.4	*1.7*	16.7	10.6
FDS	*0.2*	**13.0**	**12.0**	**47.3**	*0.8*	0.8	*0.2*	*0.2*	*0.2*	1.1	0.6	0.2	*0.0*	*0.0*	*0.0*	0.0	0.0	0.0	0.0	0.0	1.0
VDS	*10.8*	**30.4**	*14.1*	**47.3**	**54.9**	**31.5**	*15.3*	25.1	*12.1*	*17.9*	*13.1*	*17.6*	*16*	*8.9*	*10.0*	17.9	*16.6*	*7.5*	*1.3*	16.7	25.3
BCS	18.9	*11.6*	16.6	*1.0*	*19.0*	**27.2**	**22.6**	*17.5*	20.3	19.5	**25.1**	*16.0*	19.5	*9.4*	**28.5**	17.9	24.5	*4.4*	*3.8*	16.7	20.2
PPC	*19.7*	*10.4*	*12.7*	*0.6*	*10.2*	*8.8*	**33.4**	20.5	**47.0**	21.0	*8.4*	*18.3*	**26.2**	*9.1*	**33.9**	17.9	**46.2**	**68.0**	*3.6*	16.7	22.7
JO	*0.4*	**6.5**	*0.0*	*0.0*	*0.1*	*0.8*	4.0	3.7	*0.3*	*2.4*	**15.9**	**14.4**	**8.1**	**6.4**	*0.1*	4.4	*0.4*	3.7	**85.7**	**16.7**	3.5
CIO	*4.5*	**10.6**	7.7	*0.8*	*3.6*	*5.0*	*4.5*	**11.4**	*3.9*	**11.2**	6.3	**9.9**	**12.3**	**30.8**	*5.1*	**12.2**	*1.9*	4.4	*0.0*	0.0	6.4
TNP	*5.8*	*4.3*	**15.6**	*1.4*	*7.3*	**18.7**	**12.7**	8.5	*4.7*	10.6	*3.2*	7.7	10.0	*2.9*	**17.8**	13.7	9.2	3.7	*3.8*	16.7	9.1
RAS	*0.0*	0.0	0.0	0.0	0.3	0.7	**0.7**	**0.9**	*0.0*	**0.9**	*0.0*	0.0	0.5	**1.3**	0.2	**4.7**	0.2	**3.7**	0.0	0.0	0.4
WDS	*0.0*	0.0	0.0	0.0	0.4	**1.2**	*0.0*	0.2	*0.1*	**1.4**	0.0	0.0	0.6	0.7	0.9	0.3	0.0	0.0	0.0	0.0	0.3

highlighting operational inter-dependencies and actors' dual market roles.

In general, Table IV reaffirms the patterns observed in Sections IV-A and IV-B. First, Table IV provides further evidence of vendor specialization among the top 100 actors. For example, active actors in *Victim Data Sales* predominantly advertise in this category, accounting for 54.9% of the posts. This pattern is followed by *PPC/Popups Calls* (47.0%) and *Money Laundering Services* (39.6%). In addition, we see strong over-representation in both advertisements and requests for *Money Laundering Services*, *Fake/Illicit Document Services*, *Victim Data Sales*, *Job Offerings*, and *Criminal IT Infrastructure Operations*, which is indicative of clustering. In other words, among the top 100 actors, there appears to be domain specialization within stages of the TSS operations.

Second, we observed selective cross-category bundling within functionally similar product/service categories. For example, actors active in cashout services frequently cross-posted between *Money Laundering Services* and *Fake/Illicit Document Services*, but significantly under-advertised by active actors beyond cashout services. In addition, *Fake/Illicit Document Services* actors, who also advertised mainly within the same category, exhibited a strong request concentration (47.3%). This suggests that actors with expertise in forged documents developed a dual-role where they operate simultaneously as major suppliers and buyers with minimal cross-category posting behaviors. In other words, actors in the *Fake/Illicit Document Services* operate in isolation from the larger TSS marketplace ecosystem. A similar pattern is seen for luring services as well, but to a lesser degree.

Lastly, a systematic under-representation across unrelated categories indicates that actors are not engaging across the full TSS ecosystem. For example, active actors in *Fake/Illicit Document Services*, *Victim Data Sales* and *Job Offerings* are consistently under-advertising across all other product/service categories. In other words, among the top 100 actors, there were lower level of generalism, given the limited broad cross-category participation.

Beyond vendor specialization, Table IV provides insight into the dependencies of product/service categories for TSS operation. A notable cross-category posting pattern is *Victim Data Sales*. We see an over-representation in requests for cashout services by active actors in *Victim Data Sales*, while active actors in cashout services were under-represented in both advertisements and requests for *Victim Data Sales*. This asymmetry points to *Victim Data Sales* occupying complex supply chain positions where active actors in *Victim Data Sales* take on the role of suppliers while at the same time seeking financial services and forged documents necessary to monetize or operate the data they trade.

Another notable cross-category posting pattern is among active actors in the luring services. Firstly, these actors were overly advertising in technical infrastructure services. For example, actors actively posting in *PPC/Popups Calls* accounted for 26.2% of *Criminal IT Infrastructure Operations* advertisements and 46.2% of *Remote Access Services* advertisements. When looking reciprocally, the pattern stands, with active actors in technical infrastructure over-requesting for *Blasting Campaign Services* and *PPC/Popups Calls*. At the same time, active actors in the technical infrastructure services were generally under-advertising in luring services. This is especially evident when looking at the *PPC/Popups Calls-Remote Access Services* cross-posting where vendors in the former dominated the latter. This makes intuitive sense, as

call-based TSS would require remote desktop connection software to exploit the victims. This pattern suggests a coupling relationship between the two larger groups of product/service categories where luring mechanisms are tightly integrated with technical infrastructures for TSS operations.

When examining the cross-posting behaviors of active actors in *Money Laundering Services*, the findings point to organizational complexity. Specifically, active actors in *Money Laundering Services* show notable over-representation in *Job Offerings* advertisements (27.5%) and *Criminal IT Infrastructure Operations* requests (30.6%). The first relationship indicates vendors in *Money Laundering Services* are actively recruiting for labor. The latter relationship explains concurrent demand for technical infrastructure, which suggest potential need for robust back-end systems by active vendors in *Money Laundering Services*. This complexity aligns with the vendor specialization within cashout services.

D. Temporal Patterns

To further examine the cross-posting activities among the top 100 authors, we examine their posting behaviors across time. Firstly, the top 100 authors are divided into specialists and generalists. *Specialists* are actors who consistently post within one product/service category while *Generalists* refer to actors who post across different product/service categories [7]. We utilized the Sankey diagrams to systematically visualize changes in behavior patterns among the top 100 actors. Figure 1 illustrates the representative examples, where Authors 1 and 2 are *Generalists* and Authors 3 and 4 are *Specialists*.

The Sankey diagrams highlight some degree of specialization within generalists, as seen in the posting behaviors of Authors 1 and 2. Specifically, we see that Author 1 in Figure 1 focused on advertising *Victim Data Sales* at the start of their participation, and later diversifying to include *PPC/Popups Calls*. At the same time, we observed a subset of generalists establishing a dominant interest in one particular product/service category, with minor interests in other categories, as reflected by Author 2's posting behaviors. In general, posting behaviors of the generalists indicate that specialization among actors is not strictly restricted, but exists along a continuum. Among specialists, eight out of the 11 in the top 100 users focused on *Money Laundering Services* (such as Authors 3 and 4). The remaining specialists are distributed across other product/service categories, including two in *Victim Data Sales* and one in *Criminal IT Infrastructure Operations*.

Additional analysis on the top 100 users showed that 75 users contributed to the *Victim Data Sales* category, while 74 posted in the *Blasting Campaign Services* category. In particular, 64 authors were active in both categories, indicating a strong overlap in participation. This overlap may reflect a logical workflow where leads and data serve as the initial input for later processes in the TSS (e.g., email blasting service). In other words, the overlap is indicative of active users engaging in complementary categories rather than considering them as isolated activities.

V. Discussion

The study adopted a multi-dimensional approach to explore the supply-and-demand dynamics of TSS marketplaces operating through Facebook groups. By examining co-posting and cross-posting behaviors of the top 100 active actors, the analysis provides preliminary insights into how these marketplaces are structured. Consistent with earlier work [11], [13], our findings provide empirical support on partial domain specialization among actors, as indicated by diagonal dominance in the co-posting and cross-category posting behaviors. The findings highlight the top 100 actors' tendencies in developing expertise instead of diversifying across multiple product/service categories. In instances where actors go beyond their main specialization, the other product/service categories were minor or complementary. This is comparable to other criminal marketplaces where the specialization is uneven among actors [13], [15], [17].

In addition, we observed clustering within functionally similar and complementary products/services. One clustering is between data and luring services. This grouping explains the victim acquisition pipeline of: (1) data brokers assisting with victim information, (2) blasting campaign providing mass outreach, (3) PPC calls enabling in-bound call generation and (4) toll-free numbers support call-based connections with victims. The second cluster encompasses the technical infrastructure services. Actors in *Criminal IT Infrastructure Operations* category concurrently advertise in *Web Development* and *Remote Access Services*, highlighting the need for sophisticated technical back-end setup to operate TSS. These findings indicate that active actors in this TSS ecosystem tend to concentrate their activities within a relatively narrow domain, potentially reflecting the development of expertise, reputation, or resource constraints associated with specific services.

We also observed several co-posting behaviors that point to potential operational dependencies between services. For example, actors involved in victim data sales appear more likely to request cashout-related services, which may indicate downstream needs associated with monetization. Similarly, the strong co-occurrence between victim luring mechanisms (e.g., *blasting campaign services*) and infrastructure services (e.g., remote access tools) suggests that these elements may be functionally linked within TSS execution. This provides some foundational support for possible crime script pathways within TSS operations.

Taken together, the findings suggest that the marketplace is characterized by partial specialization and conditional dependencies between services. Rather than a fully integrated system in which actors manage all stages of an operation, the observed co-posting and cross-category posting behaviors point to a marketplace with a broader division of labor that is characterized by interdependent roles across different stages of TSS operations. This perspective complements prior explanations emphasizing barriers to entry and technical complexity [17], by highlighting how operational sequencing and resource inter-dependencies may further shape patterns of

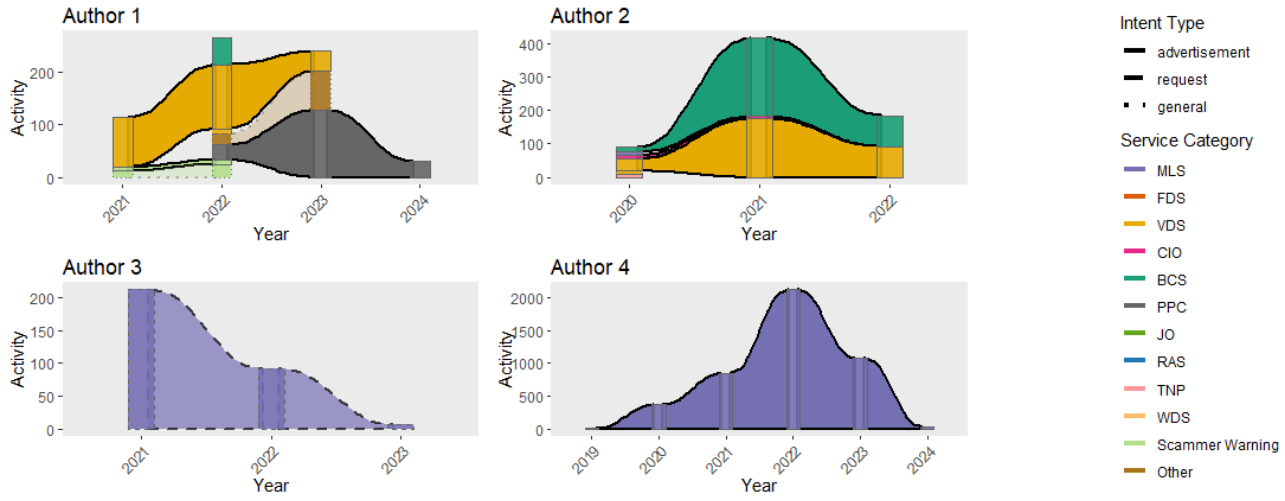

Fig. 1. Sankey diagrams of a few selected authors among the top 100 authors.

specialization. Overall, the finding suggests that the actors' roles and behaviors in the TSS marketplaces are influenced by the supply-and-demand and operational dynamic.

VI. Limitations

Several limitations merit consideration. First, the analysis is restricted to the data collected from Facebook groups. Although analogous communities operate across other platforms, the scale and activity level of Facebook provide a robust and empirical basis for analysis. Second, with the classification accuracy of 90%, a marginal proportion of false negatives may be present. In response, the analysis exclusively focused on top 100 active users, a methodological boundary imposed to reduce potential impact of misclassifications and strengthen overall reliability of findings.

Third, the analysis is performed based on public posts by actors. These posts do not indicate whether the advertisements and requests ended with completed transactions. The co-posting behaviors therefore reveal potential operational dependencies and inferred structure of marketplace rather than verified transactional networks. Finally, adoption of the NLI model reflects the hardware constraints of the research environment.

VII. Future Work

This study can be further extended in several directions. First, investigating how these supply-and-demand dynamics evolve over time will improve on current knowledge on scam tactics and strategies, which may in turn affect the dynamics of the marketplace. Second, the dataset can be expanded by incorporating data from other platforms, enabling a sophisticated understanding of TSS marketplace. Finally, future research should focus on developing empirical disruption strategies for TSS ecosystem on social media platforms.

VIII. Concluding Remarks

This research utilizes a multi-faceted approach to understand the organizational structure of TSS marketplaces. To identify the intent within the vast corpus of social media posts, we leveraged scalable analytical pipeline driven by empirical data. We automated the classification process by fine tuning a pre-trained model with the labels derived from ground truth approach. We believe that the proposed method can be effectively utilized for datasets originating from other cybercrime forums. Our analysis on buyer behavior, seller behavior, and dual marketplace roles explains significant characteristics of TSS marketplace: (1) supply-demand asymmetries provide strategic positioning, (2) functional clustering of categories based on operational dependencies, (3) supply chain role differentiation, and (4) core-marginal service structures.

References

[1] D. Harley, M. Grooten, S. Burn, C. Johnston *et al.*, "My pc has 32,539 errors: how telephone support scams really work," *Virus Bulletin*, 2012.

[2] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), "2025 Internet Crime Report," Internet Crime Complaint Center (IC3), Federal Bureau of Investigation, Tech. Rep., Apr. 2026. [Online]. Available: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

——, "2024 Internet Crime Report," Internet Crime Complaint Center (IC3), Federal Bureau of Investigation, Tech. Rep., Apr. 2025, iC3's annual report combining data from 859,532 complaints; reported losses reached $16.6billion in 2024—up 33% from 2023. [Online]. Available: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[3] S. Rauti and V. Leppänen, ""you have a potential hacker's infection": A study on technical support scams," in *2017 IEEE International Conference on Computer and Information Technology (CIT)*. IEEE, 2017, pp. 197–203.

[4] B. Srinivasan, A. Kountouras, N. Miramirkhani, M. Alam, N. Nikiforakis, M. Antonakakis, and M. Ahamad, "By hook or by crook: Exposing the diverse abuse tactics of technical support scammers," *arXiv preprint arXiv:1709.08331*, 2017.

[5] Federal Trade Commission, "How to spot, avoid, and report tech support scams," Sep. 2025, https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.

[6] R. Cherupalli, H. Grubbs, Y. T. Chua, W. Pei, T. Moore, and G. Warner, "Contextual classification of cybercriminal posts using large language models: A comprehensive study on tech support scam marketplaces," in *2025 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2025, pp. 1–11.

[8] J. Liu, P. Pun, P. Vadrevu, and R. Perdisci, "Understanding, measuring, and detecting modern technical support scams," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2023, pp. 18–38.

[9] N. Miramirkhani, O. Starov, and N. Nikiforakis, "Dial one for scam: A large-scale analysis of technical support scams," in *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society, 2017.

[10] J. Larson, B. Tower, D. Hadfield, D. Edge, and C. White, "Using web-scale graph analytics to counter technical support scams," in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018, pp. 3968–3971.

[11] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in *24th USENIX security symposium (USENIX security 15)*, 2015, pp. 33–48.

[12] M. C. Van Hout and T. Bingham, "'surfing the silk road': A study of users' experiences," *International Journal of Drug Policy*, vol. 24, no. 6, pp. 524–529, 2013.

[13] R. Van Wegberg, F. Miedema, U. Akyazi, A. Noroozian, B. Klievink, and M. van Eeten, "Go see a specialist? predicting cybercrime sales on online anonymous markets from vendor and product characteristics," in *Proceedings of the web conference 2020*, 2020, pp. 816–826.

[14] K. K. Peretti, "Data breaches: What the underground world of" carding" reveals," *Santa Clara Computer & High Tech. LJ*, vol. 25, p. 375, 2008.

[15] A. Haslebacher, J. Onaolapo, and G. Stringhini, "All your cards are belong to us: Understanding online carding forums," in *2017 APWG symposium on electronic crime research (eCrime)*. IEEE, 2017, pp. 41–51.

[16] Y. T. Chua, "Sale of private, confidential, and personal data," in *Handbook on Crime and Technology*. Edward Elgar Publishing, 2023, pp. 138–155.

[17] T. J. Holt and J. R. Lee, "A crime script analysis of counterfeit identity document procurement online," *Deviant Behavior*, vol. 43, no. 3, pp. 285–302, 2022.

[18] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent dirichlet allocation," *Journal of machine Learning research*, vol. 3, no. Jan, pp. 993–1022, 2003.

[19] R. Mihalcea and P. Tarau, "Textrank: Bringing order into text," in *Proceedings of the 2004 conference on empirical methods in natural language processing*, 2004, pp. 404–411.

[20] B. Pang and L. Lee, *Opinion mining and sentiment analysis*. Now Publishers Inc, 2008.

[21] I. Dagan, O. Glickman, and B. Magnini, "The pascal recognising textual entailment challenge," in *Machine learning challenges workshop*. Springer, 2005, pp. 177–190.

[22] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," in *Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers)*, 2019, pp. 4171–4186.

[23] Y. Liu, M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov, "Roberta: A robustly optimized bert pre-training approach," *arXiv preprint arXiv:1907.11692*, 2019.

[24] P. He, X. Liu, J. Gao, and W. Chen, "Deberta: Decoding-enhanced bert with disentangled attention," *arXiv preprint arXiv:2006.03654*, 2020.

[25] L. Fei-Fei, R. Fergus, and P. Perona, "One-shot learning of object categories," *IEEE transactions on pattern analysis and machine intelligence*, vol. 28, no. 4, pp. 594–611, 2006.

[26] O. Vinyals, C. Blundell, T. Lillicrap, D. Wierstra *et al.*, "Matching networks for one shot learning," *Advances in neural information processing systems*, vol. 29, 2016.

[27] M. Laurer, W. van Atteveldt, A. Casas, and K. Welbers, "Building Efficient Universal Classifiers with Natural Language Inference," Dec. 2023, arXiv:2312.17543 [cs]. [Online]. Available: http://arxiv.org/abs/2312.17543

[28] J. Cohen, "A coefficient of agreement for nominal scales," *Educational and psychological measurement*, vol. 20, no. 1, pp. 37–46, 1960.

[29] J. M. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative sociology*, vol. 13, no. 1, pp. 3–21, 1990.

[30] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," *Journal of big data*, vol. 6, no. 1, p. 27, 2019.

[31] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "Smote: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.

[32] P. Hensman and D. Masko, "The impact of class imbalance on convolutional neural networks," *Machine Learning and Applications*, 2015.

[33] U.S. Customs and Border Protection, "Ctpat's warning indicators for trade based money laundering and terrorist financing," U.S. Department of Homeland Security, Report, July 2025.

APPENDIX A
RESULTS OF FINE-TUNED NLI MODEL

TABLE V
PERFORMANCE METRICS OF NLI MODEL

Metric	**Precision**	**Recall**	**F1**
Advertisement	1.00	0.87	0.93
Request	0.76	1.00	0.86
General	0.42	1.0	0.60
Accuracy			0.90
Macro Average	0.73	0.95	0.80
Weighted Average	0.94	0.90	0.91