ANNEX III – A duty of care standard for E-Commerce platforms

Duty of Care for E-Commerce platforms
A Standard for Removing and Preventing Counterfeit on E-Commerce Platforms

Carsten Ullrich / REACT
Revised and abridged version – August 2020
For inclusion in PhD Dissertation

A. Introduction

This document proposes a standard approach for e-commerce platforms to remove and prevent IP infringing content and unsafe or illegal products. E-commerce platforms worldwide routinely deploy reactive Notice and Takedown (NTD) processes, which allow brand owners to inform platforms of infringing or illegal around the world. In many jurisdictions, the existence of these reactive systems protects platforms against liabilities for unlawful content offered by their parties via their sites. There is, however, considerable legal ambiguity over the scope of proactive measures platforms should take to help stem the continuing flood of IP infringements and unlawful products in e-commerce.

Online platforms, including in e-commerce, have become important gatekeepers, enabling users to interact and sell on the internet. However, their business models increasingly rely not just on intermediating between users but on analysing and monetising massive amounts of traffic and content data left by these users. Their participation in and control over the activity conducted via their systems has therefore increased steadily over recent years.

In the area of e-commerce, where counterfeit sales conducted via online marketplaces remain a serious problem, this provides an economic, technological and moral justification for charging these actors with more responsibilities. These responsibilities should go beyond the current mandatory NTD obligations, and include preventive and transparency responsibilities. These responsibilities should be seen as a duty of care, along the lines of corporate responsibility, in which platforms cooperate in overall efforts to stop the infringement of intellectual property rights.

Section B constitutes the core of this document. This section defines the duties, which an e-commerce marketplace should fulfil in order to identify and mitigate the highest risks of IP infringement on its platform. Using a risk management system, the platform would need to put processes in places to identify, analyse and evaluate the counterfeit risks emanating from sellers, products and its specific business model. A number of non-exhaustive typical risk drivers are being listed for which the platform would need to perform a risk assessment. Subsequently, control measures are being listed which the platform should put in place to mitigate the highest counterfeit risks. Section C provides an overview of the technical and organisation capabilities a platform would need to have in place in order to be seen as a responsible corporate actor. Additional risk drivers and control measures are listed in ANNEX I. For completeness, common criteria for an effective and accountable NTD systems are proposed in Section C.

Section D will summarise the transparency reporting requirements that should be in place so that all users can verify the platforms' efforts. The data reported should be consistent across different all actors so as to ensure comparability. Finally, confidential reports should be made available to brand owners and public authorities. These reports should provide detail about the effectiveness of the duty of care measures put in place by platforms. They should also give detail about the automated removal decisions and provide information on system audits, corrective actions and cooperation with law enforcement.

1. Principles

The following principles should be followed when applying the duty of care measures and risk management actions proposed in this document. They are based on principles which are already applied and widely used in existing international standards.

Create and protect value*

The duty of care standard contributes to the demonstrable achievement of objectives and improvements in legal and regulatory compliance, reputation, governance, public acceptance, health and safety.

Be part of decision-making*

The duty of care measures help decision makers to make informed choices, prioritize actions and identify alternative actions.

Accountability*

Ensure that there is accountability, authority and competence to manage the processes. This includes ensuring risk controls are effective, efficient and adequate. This can be done by identifying risk owners, performance measurement and external/internal reporting, escalation processes and recognition at all levels.

Accuracy, quality & using the best information available*

The duty of care approach is informed by hard data, experience, stakeholder feedback, forecasts and expert judgement. Account should be taken of data and modelling limitations.

Collection limitation / proportionality**

Any personal information should not be collected indiscriminately. Both the amount and the type of personal information collected should be limited to that which is necessary.

Be dynamic, iterative, and responsive to change*

The risk management system continually senses and responds to change. Risks may emerge, change or disappear as external and internal events occur, context and knowledge change. Risks are continuously being monitored and reviewed.

Security/Privacy***

Ensure all systems have anti-fraud mechanisms in place to protect data from internal and external fraud. Ensure all systems protect the personal data of users.

.*ISO 31000:2009 Risk Management

** ISO 29100:2011 Information Technology – Security Techniques – Privacy Framework

*** ISO 20488:2018 Online consumer reviews

B. *Duty of care: risk assessment, prevention and removal*

1. Methodology: risk-based approach

This section proposes a risk-based approach towards the identification and prevention of counterfeit and otherwise infringing sales. According to this, e-commerce platforms have duties of care to effectively address activities and features of their business model that pose a high counterfeit risk. The definition of risk as the *effect of uncertainty on objectives* (ISO 31000) implies a preventive approach. This section will lay down actions which can be reasonably expected of an online marketplace today (duty of care) in order to assess and control the highest risk of counterfeit emanating from its business model.

The risk management actions proposed draw on principles and processes laid down in international standards ISO 31000 (Risk management), ISO 9000 (Quality management). It also draws on the recent ISO 204888 (Online consumer reviews). Given the limited time and scope of this project there will not be any more detailed and structured references to these standards.

The risk-based approach is an ongoing process. It is expected that companies identify and evaluate risk drivers on an ongoing basis and every time a new business or design feature is deployed. As an example, this can include the launch of a new product category, new categories of sellers, new target markets. Other designs and architecture features may relate to the possibility for sellers to provide product information, the way customers are allowed to comment on sellers and products, the way products and services are being recommended, the payment services on offer or the possibility of sellers of buying sponsored listings etc.

2. Risk assessment

I. Harms definition

- Economic harms

Counterfeit products violate the economic rights of trademark owners. [Here empirical data may be inserted about the economic damage caused by the sale of counterfeit products online]. The ongoing and continued violation trademark rights impacts on the exercise of the fundamental right to protection of intellectual property as guaranteed by Article 17 (2) of the Charter of Fundamental Rights of the European Union.

- Consumer protection

Counterfeit products may pose serious risks for consumer health. The sale of unsafe or illegal may also have negative consequences for the health and safety of consumers.

II. Risk identification & definition

This standard addresses the risk of the platform being used for the sale of counterfeit and illicit products. Definition of the risks that this duty of care standard addresses:

- Use of platform for counterfeit sales
- Use of platform for sales of unsafe / illegal products

III. Risk analysis

a. Risk drivers

A platform should be able to establish risk drivers (or risk factors) which impact its exposure to the risks and the causation of harms. These risk drivers are related to three broader categories.

a) The platform needs to establish and document risk drivers related to its **business model**. A non-exhaustive list of optional risk drivers is proposed under ANNEX I.
b) The platform needs to establish and document risk drivers relating to **sellers/advertisers**. A non-exhaustive list of basic (required) and optional risk drivers is proposed under ANNEX I.
c) The platform needs to establish and document risk drivers related to **products.** A non-exhaustive list of basic (required) and optional risk drivers is proposed under ANNEX I.

Figure C1 provides a list of common counterfeit risk drivers (or risk factors) which a responsible e-commerce platform can be expected to manage proactively.

A non-exhaustive overview of basic (duty of care) and additional (best practice) risk drivers, analytical tools and control measures high risks can be found in ANNEX I.

Figure C1: Risk drivers that e-commerce platforms can reasonably be expected to evaluate

Business model related: factors and features which can be indicative of counterfeit risk (non-exhaustive)	
Risk Driver	Problem
Platform architecture / design	Platform architecture, e.g. listings structure, product display, data requirements from sellers / information governance may impact counterfeit risk
Advertising	Advertising may change the exposure to counterfeit risk (money from counterfeit listings pages; advertising for counterfeit products)
Fulfilment service	Offering a fulfilment service may change risk exposure to counterfeit and illicit products.
Payment services	Degree of payment integration (own payment services, third party pay merchants, seller independent) may change exposure to counterfeit risk.
Recommender algorithms	Recommending products from sanctioned sellers or high risk product categories may change risk exposure to counterfeit

Seller related: factors which can be indicative of counterfeit risk (non-exhaustive)	
Risk Driver	Problem
Seller provenance	Different regions may be more susceptible to counterfeit trade than others
Seller legal status (B2C, C2C)	Private individuals and commercial sellers may pose different risks when selling on the platform
Seller sanctions - takedowns	Amount / frequency of product takedowns is correlated to seller counterfeit risk
Seller sanctions - suspensions	Amount / frequency of account suspensions is indicative of seller counterfeit risk; sellers with closed accounts may reopen accounts

Product (category) related: factors which can be indicative of counterfeit risk (non-exhaustive)	
Risk Driver	Problem
Product popularity (Red Flag knowledge)	Sales volume/popularity (e.g. high ranked, fast selling listing) may affect product counterfeit risk.
Product counterfeit exposure	Different product groups maybe more subject to counterfeits than others.
Brand exposure	Different brands may pose different counterfeit risk levels.

b. Platform capabilities

The platform should have robust analytical processes in place that allow them to generate internal data and intelligence for risk analysis and risk classification.

Platforms are expected to understand the wider risk environment in which they operate. They should draw on external intelligence from brand owners, supply chain intermediaries, industry, international organisations, government and law enforcement. Figure C2 lists the analytical tools that e-commerce marketplaces should deploy for risk analysis as part of their duty of care.

Figure C2: Risk analysis tools and capabilities which e-commerce platforms should have in place

Internal data & analytical tools	For risk driver
Takedown data analytics from NTD requests and automated/internal takedowns by: ● seller ID ● seller provenance ● seller legal status ● seller size ● seller tenure ● product group ● brand	Seller provenance Seller legal status Seller sanctions (takedowns & account suspensions) Product popularity (red flag knowledge) Product group exposure Brand exposure
Seller sanctions and suspension analytics	Seller provenance Seller legal status Product popularity (red flag knowledge)
Product sales analytics	Product group exposure Product popularity (red flag knowledge)
Price analytics (list price fluctuations, deviation from RRP)	Product popularity (red flag knowledge) Brand exposure
Keyword search tools (for customer reviews, seller ratings, product descriptions, product titles)	Product exposure Brand exposure

External data / intelligence	For risk driver
Intelligence and reports from public authorities, law enforcement, international organizations (for examples see ANNEX VI)	Seller provenance
Legal requirements applying to private and commercial sellers	Seller legal status
Industry and supply chain intermediary	Product popularity (red flag knowledge) Product group exposure Brand exposure
Brand owner information	Product popularity (red flag knowledge) Product group exposure Brand exposure

IV. Risk evaluation

Following the analysis, the counterfeit risks relating to each risk factor should be evaluated (or classified) into high, medium and low risks. The eventual risk evaluation of sellers, products and business model should take into account the risk scores across all factors.

a) **Seller risk:** the platform should establish risk profiles for sellers by taking into account how the sellers scores across different risk drivers.
b) **Product risk:** the platform should establish risk levels for each product group by taking into account the exposure to risk drivers.
c) **Business model risk:** the platform should establish the counterfeit risk levels of specific features of its platform design and business model.

Platforms should have documented and transparent processes in place to evaluate risk and determine high risks. They should establish for each risk driver criteria or thresholds for risk levels (usually low, medium or high risks). The risk evaluation can for example be documented in a risk matrix (see for examples in ANNEX IV).

These processes must be validated by the management and fit into the wider counterfeit and overall risk management strategy of the company. They need to be regularly reviewed and audited.

3. Risk control

Platforms should adopt a graduated approach that corresponds to the risk level.

This standard puts an emphasis on the risk response measures adopted to<u> high counterfeit risks</u>. These should be dealt with as a priority and resources should be concentrated on these risks.

Risks at all levels should be monitored continuously in order to identify trends which could lead to a change in risk level.

A number of <u>risk mitigation</u> and <u>risk avoidance</u> measures are proposed in order to control high counterfeit risks.

For example, sellers, product and brands which display high risk indicators should be subject to enhanced due diligence checks during onboarding (KYC) and enhanced transaction and account review procedures during their tenure and lifecycle on the platforms.

Reviews should be largely automated, but need to be supplemented by regular human reviews. Human reviews are needed in order to verify systems decision accuracy and decide in non-standard situations. They will also be useful to enhance and adjust automated systems based on artificial intelligence.

In order to be able to conduct enhanced controls of high risks the e-commerce platform would need to have in place basic investigative resources and capabilities, listed in Figure C3.

Figure C3: Basic risk analysis tools and capabilities that are needed in order to control high risks

Duty of care: proactive processes – platform capabilities for high risks	Comment
Robust onboarding / KYC procedures, including: ● ID / (business) address verification, tax registration	
Automated and manual systems and processes capable of: ● managing and analysing seller population ● registering and analysing transactions ● reviewing and investigating seller accounts (requesting and verifying documents, such as invoices or authorizations) ● registering and analysing takedowns and suspensions ● detecting and verifying relation to other accounts ● conducting and analysing keyword searches of customer reviews, seller ratings, product titles and product descriptions ● reviewing and investigating listing authenticity (requesting and verifying documents, such as invoices or authorizations, incorporating feedback from supply chain intermediaries and brand owners)	These actions can be assured through a team of trained reviewers or investigators for example as part of existing fraud / risk management. The processes can be documented through standard operating procedures, or by providing training materials, for example based on brand or industry intelligence.
Regular audit and review of sellers, product group and brands': ● risk categorizations ● risk evaluation criteria	

With these capabilities in place, platforms are in a position to design control measures in order to address the high risks of counterfeits (Figure C4). These measures would be at the core of the duty of care of on online marketplaces.

Figure C4: Control measures for high risks as part of a duty of care

Duty of care: control measures for high risks	Risk driver	Comment
Onboarding: enhanced due diligence checks / KYC for: ● sellers from high risk regions/countries ● commercial sellers	Seller provenance Seller legal status	Combine with internal anti-money laundering procedures (KYC, risk profiling) as possible
Onboarding: check new sellers for relations with suspended accounts	Seller sanctions - suspensions	
Onboarding: enhanced authorization requirements for selling in high-risk product groups / categories	Product popularity (red flag knowledge) Product group exposure Brand exposure)	This could include enhanced information and training regarding compliance with applicable laws and T&Cs, sample invoice checks, feedback brand owners.
Enhanced automated and manual monitoring of: ● transactions of sellers from high risk regions/ countries ● transactions, customer reviews, seller ratings, product titles from sellers with a takedown history ● transactions, customer reviews, seller ratings, product titles, account relations of previously suspended sellers ● product listings (titles, descriptions, price points) in high risk product categories ● listings from high risk brands (keyword searches, price points, images) ● popular ("viral") product sales (keyword searches, price points, images) ● listings uploads of high-risk sellers, brands, in high-risk product categories product	Seller provenance Seller legal status Seller sanctions - takedowns Seller sanctions – suspensions Product popularity (red flag knowledge) Product group exposure Brand exposure)	Enhanced monitoring would include: reviews for suspicious or unusual transactions, systems to prevent re-upload of blocked listings, reviewing suspicious account movements and alterations, keyword searches in product titles and descriptions, customer reviews and seller ratings, invoice checks, product document reviews, image reviews, price point feedback from brands/ manufacturers.
A documented strike policy for listings takedowns and account suspensions/closures. (example ANNEXII)	Seller sanction –takedowns and suspension.	
Automated or manual processes to detect and enforce private seller legal thresholds for selling.	Seller legal status	

ANNEX I contains a full overview of all drivers for seller, product and business model related counterfeit risks, the processes and data needed to establish risk levels and control measures for high risks.

C. Duty of care: Notice-and-Takedown

In most jurisdictions in the world e-commerce platforms' liabilities with regards to unlawful information hosted from third parties is limited to failure to comply with reactive removal obligations. These removal obligations are normally fulfilled by Notice – and Takedown (NTD) processes.

The REACT survey confirmed that NTD systems are in place on most platforms across the globe.

There are, however, significant variations in service levels and in procedural and transparency commitments by platforms which inhibits the effective and consistent enforcement.

The good management of NTD is an essential part of the platform's entire commitment to help fight the use of its system for unlawful activities, such as counterfeit and unsafe or illegal product sales. Following the principles of Openness and Accountability responsible and effective NTD processes should be set up in the following way.

Notice and Takedown: Duty of care requirements
Make notice forms easily available to users and brand owners
Provide clear and easy notification systems
Provide the possibility to file notices for all kinds of IP violations: trademarks (counterfeit), copyright, designs, patents.
Provide the possibility to attach additional information and proof.
Provide the possibility to notify links, including advertising) leading to infringing products or content.
Provide for the possibility to file bulk notices
Provide service level agreements (SLAS) for the decision-making on notices (removal or stay-up) - this should not exceed 48 hours.
Explain the process of notice appeals, including for automated for takedowns and provide SLAs.
Provide noticing parties information on the completion of their NTD request.

See also: BASCAP, 'Best-Practices-for-Removing-Fakes-from-Online-Platforms', 2016

D. Duty of care: transparency

1. Terms & Conditions

Platforms should make a clear and unambiguous statement of their intolerance towards the use of their platform for IP infringing and other unlawful activities in their terms and conditions (T&Cs).

Terms & Conditions: company commitments
Have a clear statement that prohibits the sale of IP infringing and other unlawful products
Clear commitment towards removing and sanctioning sellers violating this prohibition.
Inform users of the NTD process and, where appropriate, provide a separate link to relevant NTD service conditions and NTD form(s)
Inform users of the type of infringements sanctioned, including for example advertising or other links to infringing products or content, incorrect but similar product names, image violations, etc.
Inform sellers of the platform's right to cooperate with law enforcement authorities.
Inform sellers of the platform's policy on discontinuing accounts and withholding of funds in the case of illegal activity.

2. Transparency reporting

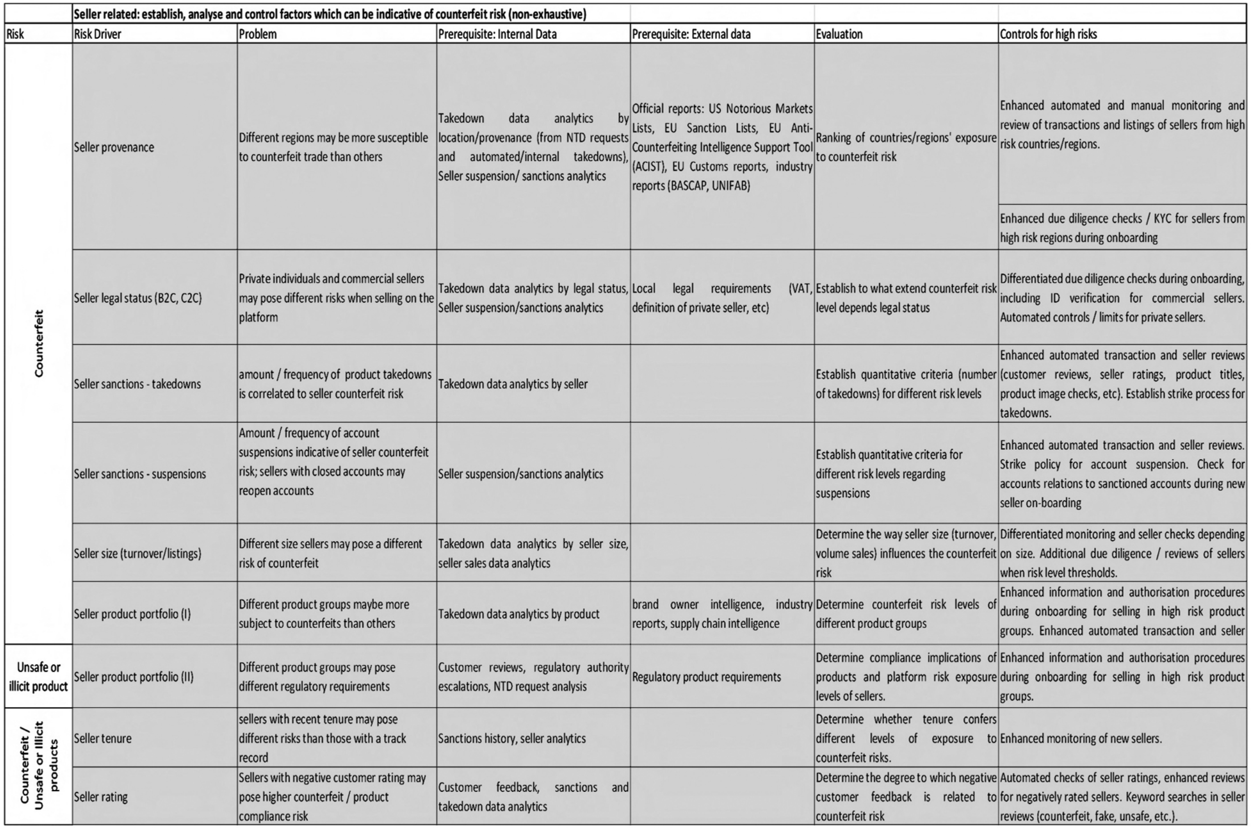
An e-commerce platform should publish a regular account of its activities in the fight against IP theft. Many platforms already publish accounts of notices and content removals, albeit in other content areas (such as hate speech). Transparency reports will ensure that the platform's commitment is visible to all stakeholders, provide accountability and help evaluate the effectiveness of the duty of care measures put in place.

Transparency reporting should be published bi-annually, but be separated into publicly available and confidential reports.

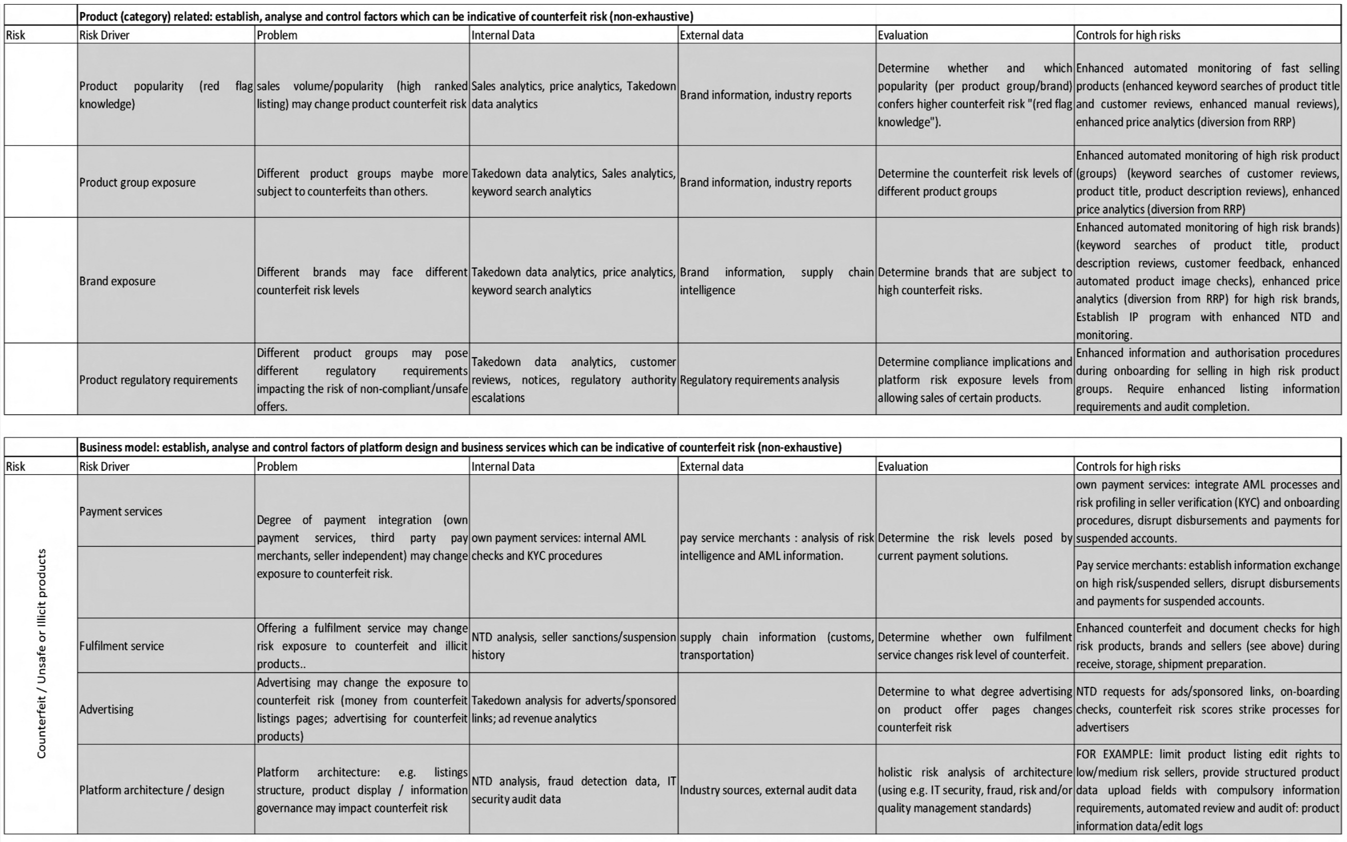
Public Transparency Reports (Bi-annual) – content
Number listing removals: NTD requests, automated removals
NTD requests: number, % of appeals, % of successful appeals, listing removals, % invalid notices
NTD requests: by type of infringement
NTD requests: by source - brand owner, seller, public authority
NTD requests: processed outside SLA (%)
Automated removals: number, % appeals, % successful appeals
Number of seller accounts closed

Confidential Transparency Reports (Bi-annual) (rightsholders/government) - content
Number of listing removals: by product category, top brands (total/product category)
Seller accounts closed by provenance (country), seller size (turnover/listings)
The number of cases referred/reported to law enforcement authorities
Activity report on: staff training, cooperation with brand owners, process audits/reviews incl. automated systems

Annex I - Management of risk drivers



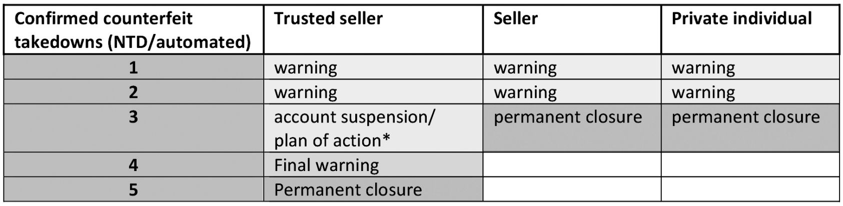
	Seller related: establish, analyse and control factors which can be indicative of counterfeit risk (non-exhaustive)					
Risk	Risk Driver	Problem	Prerequisite: Internal Data	Prerequisite: External data	Evaluation	Controls for high risks
Counterfeit	Seller provenance	Different regions may be more susceptible to counterfeit trade than others	Takedown data analytics by location/provenance (from NTD requests and automated/internal takedowns), Seller suspension/ sanctions analytics	Official reports: US Notorious Markets Lists, EU Sanction Lists, EU Anti-Counterfeiting Intelligence Support Tool (ACIST), EU Customs reports, industry reports (BASCAP, UNIFAB)	Ranking of countries/regions' exposure to counterfeit risk	Enhanced automated and manual monitoring and review of transactions and listings of sellers from high risk countries/regions.
						Enhanced due diligence checks / KYC for sellers from high risk regions during onboarding
	Seller legal status (B2C, C2C)	Private individuals and commercial sellers may pose different risks when selling on the platform	Takedown data analytics by legal status, Seller suspension/sanctions analytics	Local legal requirements (VAT, definition of private seller, etc)	Establish to what extend counterfeit risk level depends legal status	Differentiated due diligence checks during onboarding, including ID verification for commercial sellers. Automated controls / limits for private sellers.
	Seller sanctions - takedowns	amount / frequency of product takedowns is correlated to seller counterfeit risk	Takedown data analytics by seller		Establish quantitative criteria (number of takedowns) for different risk levels	Enhanced automated transaction and seller reviews (customer reviews, seller ratings, product titles, product image checks, etc). Establish strike process for takedowns.
	Seller sanctions - suspensions	Amount / frequency of account suspensions indicative of seller counterfeit risk; sellers with closed accounts may reopen accounts	Seller suspension/sanctions analytics		Establish quantitative criteria for different risk levels regarding suspensions	Enhanced automated transaction and seller reviews. Strike policy for account suspension. Check for accounts relations to sanctioned accounts during new seller on-boarding
	Seller size (turnover/listings)	Different size sellers may pose a different risk of counterfeit	Takedown data analytics by seller size, seller sales data analytics		Determine the way seller size (turnover, volume sales) influences the counterfeit risk	Differentiated monitoring and seller checks depending on size. Additional due diligence / reviews of sellers when risk level thresholds.
	Seller product portfolio (I)	Different product groups maybe more subject to counterfeits than others	Takedown data analytics by product	brand owner intelligence, industry reports, supply chain intelligence	Determine counterfeit risk levels of different product groups	Enhanced information and authorisation procedures during onboarding for selling in high risk product groups. Enhanced automated transaction and seller
Unsafe or illicit product	Seller product portfolio (II)	Different product groups may pose different regulatory requirements	Customer reviews, regulatory authority escalations, NTD request analysis	Regulatory product requirements	Determine compliance implications of products and platform risk exposure levels of sellers.	Enhanced information and authorisation procedures during onboarding for selling in high risk product groups.
Counterfeit / Unsafe or Illicit products	Seller tenure	sellers with recent tenure may pose different risks than those with a track record	Sanctions history, seller analytics		Determine whether tenure confers different levels of exposure to counterfeit risks.	Enhanced monitoring of new sellers.
	Seller rating	Sellers with negative customer rating may pose higher counterfeit / product compliance risk	Customer feedback, sanctions and takedown data analytics		Determine the degree to which negative customer feedback is related to counterfeit risk	Automated checks of seller ratings, enhanced reviews for negatively rated sellers. Keyword searches in seller reviews (counterfeit, fake, unsafe, etc.).



	Product (category) related: establish, analyse and control factors which can be indicative of counterfeit risk (non-exhaustive)					
Risk	Risk Driver	Problem	Internal Data	External data	Evaluation	Controls for high risks
	Product popularity (red flag knowledge)	sales volume/popularity (high ranked listing) may change product counterfeit risk	Sales analytics, price analytics, Takedown data analytics	Brand information, industry reports	Determine whether and which popularity (per product group/brand) confers higher counterfeit risk "(red flag knowledge").	Enhanced automated monitoring of fast selling products (enhanced keyword searches of product title and customer reviews, enhanced manual reviews), enhanced price analytics (diversion from RRP)
	Product group exposure	Different product groups maybe more subject to counterfeits than others.	Takedown data analytics, Sales analytics, keyword search analytics	Brand information, industry reports	Determine the counterfeit risk levels of different product groups	Enhanced automated monitoring of high risk product (groups) (keyword searches of customer reviews, product title, product description reviews), enhanced price analytics (diversion from RRP)
	Brand exposure	Different brands may face different counterfeit risk levels	Takedown data analytics, price analytics, keyword search analytics	Brand information, supply chain intelligence	Determine brands that are subject to high counterfeit risks.	Enhanced automated monitoring of high risk brands) (keyword searches of product title, product description reviews, customer feedback, enhanced automated product image checks), enhanced price analytics (diversion from RRP) for high risk brands, Establish IP program with enhanced NTD and monitoring.
	Product regulatory requirements	Different product groups may pose different regulatory requirements impacting the risk of non-compliant/unsafe offers.	Takedown data analytics, customer reviews, notices, regulatory authority escalations	Regulatory requirements analysis	Determine compliance implications and platform risk exposure levels from allowing sales of certain products.	Enhanced information and authorisation procedures during onboarding for selling in high risk product groups. Require enhanced listing information requirements and audit completion.

	Business model: establish, analyse and control factors of platform design and business services which can be indicative of counterfeit risk (non-exhaustive)					
Risk	Risk Driver	Problem	Internal Data	External data	Evaluation	Controls for high risks
Counterfeit / Unsafe or Illicit products	Payment services	Degree of payment integration (own payment services, third party pay merchants, seller independent) may change exposure to counterfeit risk.	own payment services: internal AML checks and KYC procedures	pay service merchants : analysis of risk intelligence and AML information.	Determine the risk levels posed by current payment solutions.	own payment services: integrate AML processes and risk profiling in seller verification (KYC) and onboarding procedures, disrupt disbursements and payments for suspended accounts.
						Pay service merchants: establish information exchange on high risk/suspended sellers, disrupt disbursements and payments for suspended accounts.
	Fulfilment service	Offering a fulfilment service may change risk exposure to counterfeit and illicit products..	NTD analysis, seller sanctions/suspension history	supply chain information (customs, transportation)	Determine whether own fulfilment service changes risk level of counterfeit.	Enhanced counterfeit and document checks for high risk products, brands and sellers (see above) during receive, storage, shipment preparation.
	Advertising	Advertising may change the exposure to counterfeit risk (money from counterfeit listings pages; advertising for counterfeit products)	Takedown analysis for adverts/sponsored links; ad revenue analytics		Determine to what degree advertising on product offer pages changes counterfeit risk	NTD requests for ads/sponsored links, on-boarding checks, counterfeit risk scores strike processes for advertisers
	Platform architecture / design	Platform architecture: e.g. listings structure, product display / information governance may impact counterfeit risk	NTD analysis, fraud detection data, IT security audit data	Industry sources, external audit data	holistic risk analysis of architecture (using e.g. IT security, fraud, risk and/or quality management standards)	FOR EXAMPLE: limit product listing edit rights to low/medium risk sellers, provide structured product data upload fields with compulsory information requirements, automated review and audit of: product information data/edit logs

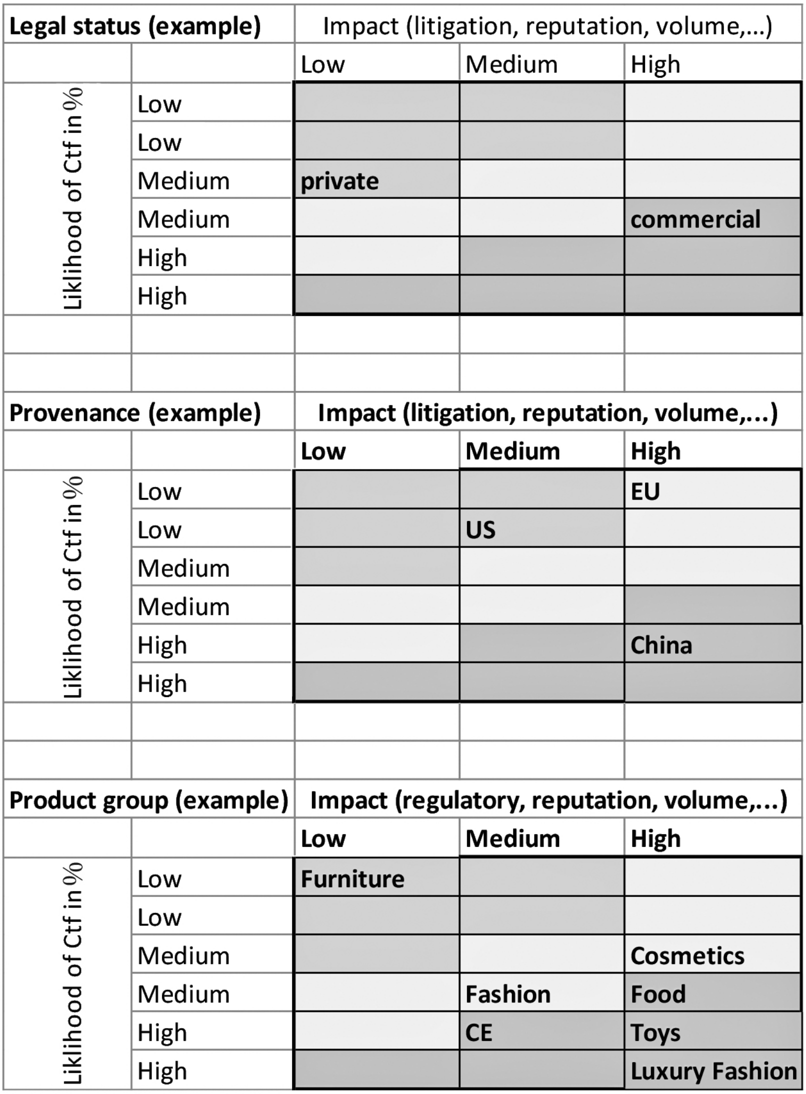
Annex II - IP Infringement Strike Policy (Example)



Confirmed counterfeit takedowns (NTD/automated)	Trusted seller	Seller	Private individual
1	warning	warning	warning
2	warning	warning	warning
3	account suspension/ plan of action*	permanent closure	permanent closure
4	Final warning		
5	Permanent closure		

**Plan of Action/account suspension: the seller is contacted by the platform and asked to provide reasons for the occurrence of counterfeit (infringing) products. They would need to commit to actions in order to prevent the sale of counterfeit. A temporary account suspension would be imposed (e.g. 1 month) during which the seller will have to implement these actions.*

Annex III – Risk Matrix (examples)



Legal status (example)		Impact (litigation, reputation, volume,…)		
		Low	Medium	High
Liklihood of Ctf in %	Low			
	Low			
	Medium	**private**		
	Medium			**commercial**
	High			
	High			
Provenance (example)		**Impact (litigation, reputation, volume,...)**		
		Low	**Medium**	**High**
Liklihood of Ctf in %	Low			**EU**
	Low		**US**	
	Medium			
	Medium			
	High			**China**
	High			
Product group (example)		**Impact (regulatory, reputation, volume,...)**		
		Low	**Medium**	**High**
Liklihood of Ctf in %	Low	**Furniture**		
	Low			
	Medium			**Cosmetics**
	Medium		**Fashion**	**Food**
	High		**CE**	**Toys**
	High			**Luxury Fashion**

Annex IV – Public Reports and Data Sources

Europol and EU Intellectual Property Office, '2017 Situation Report on Counterfeiting and Piracy in the European Union' (2017)

Frontier Economics, ‘The Economic Impacts of Counterfeiting and Piracy - Report Prepared for BASCAP and INTA’.

Office of the United States Trade representative, ‘2017 Out-of-Cycle Review of Notorious Markets’w