Table of Contents

1. Introduction 3

2. Risk Assessment mechanisms and methodology 6

2.1 Amazon's mechanisms for risk assessment 6
2.2 Risk Assessment methodology 6
2.3 Risk assessment and management in AI implementation 7

3. Assessment of Illegal Content Risk 8

3.1 Seller verification 10
3.2 Brand protection 10
3.2.1 Robust proactive controls 12
3.2.2 Powerful tools to support brand protection 13
3.2.3 Holding bad actors accountable 14
3.2.4 External engagement and education 15
3.3 Product safety and compliance 17
3.3.1 Robust proactive controls 19
3.3.2 Powerful tools to support product safety 20
3.3.3 Holding bad actors accountable 22
3.3.4 External engagement and education. 22
3.4 Trustworthy customer reviews 23
3.4.1 Robust proactive controls 24
3.4.2 Powerful tools to support trustworthy reviews 25
3.4.3 Holding bad actors accountable 25
3.4.4 External engagement and education 27
3.5 Advertising and recommender systems in the Amazon EU Store 28
3.5.1 Advertising in the Amazon EU Store 28
3.5.2 Recommender systems in the Amazon EU Store 31
3.6 Measures to prevent reappearance of illegal content 32
3.7 A-to-z guarantee and return policy 33

4. Assessment of Fundamental Rights Risk 33

4.1 Consumer protection 35
4.2 Offensive and controversial products 35
4.2.1 Proactive controls 36
4.2.2 Mechanisms to moderate offensive and controversial products 36
4.2.3 Holding bad actors accountable 37
4.2.4 Preventing amplification 37
4.3 Fair and objective moderation of content in the Amazon EU Store 37
4.3.1 Proportionate proactive controls 37
4.3.2 Transparent content moderation tools 38
4.3.3 Fair enforcement and redress 38
4.3.4 Educating Sellers 39
4.4 Maintaining customer trust through privacy 39
4.4.1 Risk assessment and mitigation steps 39
4.5 Helping Sellers to conduct their business 42

5. Assessment of Democratic Process Risk 44
6. Assessment of Public Health Risk 44
7. Conclusion 46

1. Introduction

Founded in 1994, Amazon started as an online retailer for books. In 2001, Amazon opened its store to third-party selling partners ("**Sellers**"). Today, Amazon operates the Amazon stores where customers can find a wide range of products including books, clothes, electronic equipment, car accessories, kitchen and home appliances, toys and many more products on different country-specific online interfaces. Amazon serves its customer-centric mission by striving to provide customers with the best combination of selection, price, and customer experience to make sure customers are satisfied with their shopping experience, including their purchase.

The Amazon EU Store is run as a single store that makes products from Sellers available for purchase ("**Amazon Marketplace**") as well as Amazon's own retail offers. It is operated by **AEU**. Amazon's own retail activities ("**Amazon Retail**") are also conducted by AEU, and Amazon Europe Core S.à.r.l. acts as technical service provider operating the websites, tools, and data infrastructures. AEU provides Amazon Marketplace services to Sellers enabling them to offer products for sale in the Amazon EU Store. AEU generates revenues by charging commissions on the transactions it facilitates. Amazon Marketplace connects Sellers and end customers, who shop in the Amazon EU Store.

The Amazon EU Store is local and physical in nature. It is operated through distinct digital storefronts with top-level domain names in Germany, France, Italy, Spain, the Netherlands, Poland, Belgium, Sweden and Ireland (each a "**Storefront**").

Amazon is first and foremost a retail store operator. As such, providing a trustworthy shopping experience for all its users is the cornerstone of its business model. As Amazon operates in an intensely competitive and highly fragmented retail landscape, where a plethora of retail channels are available to customers and Sellers, mitigating potential risks to those users has always been a central tenet of its operations.

Customers have many options for purchasing, and stores compete fiercely for their business. Amazon has long recognized that one of the fundamental factors that guides customer choice is trust. If customers do not trust Amazon, they will simply shop elsewhere. Amazon's goal is therefore to offer products and operate a store that provides customers with the most trustworthy shopping experience. As advertising in Amazon's stores is merely in service of products sold in those stores, it has no incentive to display content that seeks merely to retain customer attention, including illegal or abusive content. In fact, such content would have the contrary effect: it would harm Amazon's reputation, diminish the likelihood of repeat purchases, and steer customers and Sellers to Amazon's competitors.

Customers who visit a Storefront have a number of options to find products in the Amazon catalogue, for example by browsing the Amazon EU Store and product categories, entering a shopping query, or clicking on paid advertising. Both Amazon Retail and Sellers can create listings in the Amazon catalogue. The "product detail page", which is the name we give to the common detail page for each unique listing, is populated by Amazon as store owner with information from various sources, which could include Amazon Retail, brand owners, and Sellers. Once a new product listing is created in the Amazon catalogue, Sellers can simply add offers for that product so that customers can easily find and compare offers. All offers are presented on a product detail

page in a consistent and unified way for customers with a view to facilitating their shopping journey. Amazon has found that it is key to provide customers with a single standardized source for product information, reviews, and competing offers in the store, so that they can easily compare all offers for a product and make a purchase. The logic of our single store is reflected in the single product detail page.

Users, including customers and regulators, can clearly identify the Sellers of each product listed in the Amazon EU Store. Users can find information about the Seller of each product on the product detail page. On this page, users can click to view detailed information about the Seller, including the Seller's name, address, and trade register information that is provided through the Seller verification process (described in more detail in Section 3.1 below). Users are able to contact Sellers directly through our "Ask a question" functionality on the Seller profile page.

It is also essential for Amazon's success to maintain Sellers' and brands' trust over the long term, and to ensure that they too have a high-quality experience. As approximately two thirds of the orders placed on Amazon are for Sellers' products, Amazon succeeds when Sellers succeed. Thus, Amazon tailors its measures and tools when managing its relationship with Sellers to deter unwanted or unlawful behavior, on the one hand, and ensure Seller trust, on the other. Amazon cooperates closely with Sellers to understand the problems that have given rise to potential risks, educate them on how to comply with the law, and assess both over- and under-enforcement through its programs and tools. Amazon's objective is to prevent bad actors and illegal, non-complaint or unsafe products from entering our store, and to continuously monitor and listen to signals that indicate if a bad product or bad actor has made it into our store, learning from these events to prevent them from happening in the future.

Reflecting this commitment to both customers and Sellers, risks that could potentially arise and negatively impact customers' and Sellers' experiences and expectations are constantly identified, assessed, and managed in the ordinary course of the Amazon EU Store's business, not just in the context of this Risk Assessment. In addition, due to the novel obligations imposed on Amazon by Article 34 of the DSA, Amazon has made an in-depth re-assessment of its existing risk assessment and mitigation controls to take sufficient account of the specific requirements of the DSA's Systemic Risk Categories.

We consider that the risks identified in the DSA which might be relevant for Amazon are already mitigated effectively through measures which are comprehensively integrated into Amazon's daily work, operations, and governance structures. Amazon has consistently been a leader in developing new programs and tools against any form of abuse relevant to its business model. The development and implementation of these measures has a long history, which precedes the entry into force of the DSA by some time. Throughout our 30 years of operations, Amazon has voluntarily implemented "reasonable, proportionate and effective mitigation measures", as required under Article 35(1) of the DSA, to counter any risks that are relevant to the Amazon EU Store. It has done so through careful and detailed analysis, and sustained and proactive investment in people and technologies. These risk analyses and mitigation measures are integral to Amazon's business model, which is founded on customer trust and confidence in its store. For years, they have been tailored to Amazon's particular business model: a retailer with the goal of being Earth's most customer-centric company.

As will be reflected in the analysis of the Systemic Risk Categories we set out below, Amazon's overall strategy to protecting the Amazon EU Store from risk of all forms of abuse centers on four strategic areas. These four strategic areas frame the reasonable, proportionate, and effective measures Amazon has implemented to mitigate negative effects of the Systemic Risk Categories for users of the Amazon EU Store. Our approach to trust and safety is built on five key areas. We are constantly innovating and improving across these areas to protect our customers.

1. **Robust proactive controls**. Our robust proactive controls use advanced machine learning techniques and automation to continuously monitor all aspects of the Amazon EU Store for fraudulent, infringing, inauthentic, non-compliant or unsafe products. From the moment a Seller attempts to register, our advanced technology continually scans for potential fraud and abuse, and continues to do so as future changes are submitted. We use the data and learnings gathered from these technologies to innovate and improve our proactive controls.

2. **Powerful tools to protect the Amazon EU Store**. The Amazon EU Store is designed and functions to support Sellers offering authentic, safe products. We provide powerful tools enabling Sellers to understand and comply with applicable product compliance requirements. In addition, we offer industry leading tools to enable brands to manage and protect their brand and intellectual property rights ("**IP**"), on and off Amazon.

3. **Holding bad actors accountable**. When Amazon identifies abuse or misuse of the Amazon EU Store, we act quickly to protect customers, brands and Sellers by removing infringing, or unsafe products, blocking bad actor accounts, and referring cases to law enforcement to mitigate risks across the supply chain. We also pursue civil suits, and work with law enforcement on joint enforcement and seizures across the globe. This deters and prevents bad actors from selling infringing, counterfeit or unsafe products on the Amazon EU Store (and indeed from other retailers' stores).

4. **Protecting and educating customers**. Our robust proactive controls protect customers while they shop on the Amazon EU Store, but we don't stop there. We provide customers with information they need to protect themselves from bad actors and extend this work through collaboration with public and private sector organizations helping create a more trustworthy shopping experience everywhere.

5. **Collaborating across industry.** We regularly engage with consumer advocacy organizations, governments, regulators, academia, and others who share our commitment to protecting consumers and small businesses. Through these collaborations, we work to identify emerging risks, share best practices, and develop solutions that benefit customers wherever they shop. Amazon operates continuous programs to monitor and improve its performance. When Amazon identifies new problems or risk vectors, the relevant business lines implement mechanisms or closed-loop processes to define the key input and output risk metrics and assess the efficacy of mitigation measures. Business lines will set performance improvement goals on an annual basis, and track progress against those goals throughout the year. Key performance metrics are evaluated by business leadership periodically through weekly, monthly, or quarterly reviews. Where gaps are identified, relevant teams work to address and resolve them.

Through these processes, which have been adjusted and refined over many years, Amazon identifies and mitigates the potential risks it considers most relevant to the Amazon EU Store. The risk assessment process set out in Article 34(1) of the DSA is therefore, by its very nature, already embedded in Amazon's risk mitigation practices – which we consider to be fully aligned with the requirements of Article 35 of the DSA.

2. Risk Assessment mechanisms and methodology

2.1 Amazon's mechanisms for risk assessment

Amazon has developed an industry leading approach to risk assessment. Our risk assessment begins with analyzing market intelligence, industry patterns, regulatory requirements, and customer insights. We combine customer feedback, competitive analysis, and risk parameters to identify potential threats before they materialize. This comprehensive approach enables us to anticipate shifts in customer behavior, supply chain vulnerabilities, regulatory changes, and security threats that could impact the Amazon EU Store.

Our continuous monitoring system merges control mechanisms with advanced analytics for comprehensive risk management, following established industry frameworks and best practices. These systems track key risk indicators across operational, financial, compliance, and reputational dimensions. When issues arise, we conduct a thorough root cause analysis, examining immediate triggers and systemic factors that contribute to risk exposure, aligned with international standards for risk management.

We have implemented a structured risk assessment framework that evaluates compliance requirements, fraud or abuse patterns, technological vulnerabilities, and emerging threats. This framework incorporates industry best practices and is complimented by AI/ML capabilities that process transaction patterns and customer interactions to identify anomalies and predict risks. We regularly strengthen our risk controls through compliance reviews, operational assessments, and established risk management methodologies.

These strategies demonstrate Amazon's commitment to robust risk management that adapts to new and evolving risks. Our assessment techniques and controls evolve through continuous learning, innovation, and adherence to leading industry practices, ensuring comprehensive protection of our stores.

2.2 Risk Assessment methodology

The DSA framework recognizes that each VLOP requires an individualized assessment based on its unique business model and purpose. Accordingly, this Risk Assessment considers the DSA Systemic Risk Categories specific to Amazon's operations and draws from diverse sources, including customers, regulators, brands, Sellers, and authorities, as outlined in DSA Recital 90. This Risk Assessment thoroughly evaluates both actual and potential DSA Systemic Risk in the Amazon EU Store, along with the risk mitigation measures. The Risk Assessment methodology involved comprehensive consultations with operational teams and their leadership, gathering relevant data and documentation that captured changes affecting the DSA Systemic Risk Categories.

We conducted comprehensive consultations across Amazon's operational teams to assess their influence on the DSA Systemic Risk Categories. Search and recommender system teams evaluated how their design choices impact these risks, while specialized fraud and abuse mitigation teams assessed the effectiveness of content moderation systems across areas including IP infringement, product safety, customer reviews, and anti-money laundering compliance. Teams responsible for enforcing terms and conditions provided detailed input on how policies affect risk management, and the advertising team contributed analysis of advertisement placement systems' impact. Additionally, data privacy and operational teams offered insights into how data practices influence risk categories, while experts in content moderation law and human rights assessment provided broader contextual analysis. This thorough cross-functional approach enabled us to comprehensively evaluate how Amazon's systems and practices affect the DSA Systemic Risk Categories.

We also audited our feedback mechanisms to identify and assess emerging risks, particularly those with the potential to impact the DSA Systemic Risk Categories. This involved analyzing customer and Seller feedback, reviewing notice and takedown patterns, consulting with brands, collaborating with authorities, and gathering input from key stakeholders. Amazon actively tracks and measures these risks' severity and probability, which we detail below.

In the following sections, we address each of the Systemic Risk Categories under Article 34 of the DSA. The Systemic Risk Categories covered under Article 34 of the DSA includes the risks of disseminating illegal content (the "**Illegal Content Risk**"), negative effects on the exercise of fundamental rights protected by the Charter of Fundamental Rights of the European Union (the "**Fundamental Rights Risk**"), negative effects on civic discourse, electoral processes and public security (the "**Democratic Process Risk**"), and negative effects on the protection of public health and minors, serious negative consequences to a person's physical and mental wellbeing, and gender-based violence (the "**Public Health Risk**").

2.3 Risk assessment and management in AI implementation

As part of its continuous innovation, Amazon has integrated generative AI technologies ("**AI**") into select functionalities within the Amazon EU Store. These implementations aim to enhance the overall shopping experience and customer interactions while maintaining and, in some cases enhancing, Amazon's commitment to trust and safety.

Responsible AI development is non-negotiable for Amazon, and we are deeply committed to protecting the privacy and security of data across our organization.

Amazon maintains a dynamic approach, continuously updating and improving its AI risk assessment and management framework based on emerging risks and user feedback in an area of rapid technological innovation. This ensures not only compliance with DSA requirements but also upholds Amazon's fundamental commitment to customer trust and safety in an evolving digital landscape. Before any AI functionality reaches the Amazon EU Store, Amazon conducts extensive pre-deployment assessments to evaluate potential impacts on user safety and rights. Where relevant, Amazon also conducts a risk assessment process that addresses the four fundamental DSA Systemic Risk Categories: Illegal Content Risk, Fundamental Rights Risk, Democratic

Process Risk, and Public Health Risk. Each category undergoes rigorous evaluation that weighs both likelihood and severity to determine overall risk levels.

Once launched, Amazon operates on-going monitoring and early detection systems using multiple feedback channels, including the existing customer reporting mechanisms that allow users to flag concerns with content in the Store. This response capability is complemented by the review and update of safety protocols to address emerging challenges. The effectiveness of these measures is reflected in consistently low risk ratings across all systemic risk categories. Amazon also prioritizes transparency to customers when they are engaging with AI. This helps to manage expectations and maintain trust and security. In this way Amazon balances innovation with responsibility, ensuring that new AI functionalities enhance the customer experience while maintaining robust protections against potential DSA Systemic Risks.

3. Assessment of Illegal Content Risk

The continuous identification, analysis, and assessment of the risks of illegal, unsafe, or counterfeit products is integral to the success of Amazon's business. In this section we assess the risk the Amazon EU Store is abused or misused to sell illegal products, having regard to Recital 80 to the DSA which specifically includes within the Illegal Content Risk the potential risk of "*the sale of products or services prohibited by Union or national law, including dangerous or counterfeit products.*"[1]

Amazon's terms and conditions with all Sellers strictly prohibit the offer of any infringing, inauthentic, non-compliant and unsafe products, and each Seller agrees to these terms and conditions when registering to sell in the Amazon EU Store. When Sellers violate these policies, they may be subject to removal of the listing or listing content, and in more severe cases to suspension of selling account privileges. Section 4.3 provides additional information regarding the enforcement of our terms and conditions for Sellers, which contributes to Amazon's strategy to managing the Illegal Content Risk. For ease we refer in this Risk Assessment to the applicable terms, policies and guidelines for one of our Storefronts; however, substantially similar policies and guidelines apply to all of our Storefronts.

Illegal Content Risk is neither specific to nor increased for large online retailers. The types of risks that impact the Amazon EU Store, such as inauthentic and unsafe products, pre-date Amazon and are endemic to the retail industry as a whole. Therefore, Amazon identifies risk and adopts mitigations based on best practices applicable to any retailer of consumer goods, and in many cases, Amazon takes actions that go beyond industry best practices.

In fact, the risk of the sale of counterfeit or other illegal products may be more prevalent in smaller stores, as they generally have fewer resources to ensure compliance. In contrast, larger stores have greater incentives to develop and deploy measures against dangerous or illegal goods, faced with more media attention which may lead to more negative publicity and a bigger impact on reputation

[1] For completeness, Recital 80 to the DSA also mentions that Illegal Content Risk could arise from the sale of "*illegally-traded animals*". This is not applicable, as the Amazon EU Store does not sell pets. Additionally, while the Amazon EU Store in principle does not pose systemic risks related to "*dissemination of child sexual abuse material or illegal hate speech*", because such risks are associated with social media and content sharing services, measures capable of addressing any such (non-systemic) risks in the Amazon EU Store are discussed in Section 4.2 below.

and customer and seller trust compared to smaller stores. Larger stores also have more resources to develop more know-how and more effective tools to fight trade in illegal goods. In 2024, Amazon invested more than a billion dollars and employed thousands of people including machine learning scientists, software developers, and expert investigators who were dedicated to protecting customers, brands, selling partners, and our store from counterfeit, fraud, and other forms of abuse. In addition, to the extent there are industry-level risks that exist in the retail sector, the sector has been regulated for many years with a view to mitigating these risks, both through government and self-regulation, including in relation to online sales (*e.g.*, pursuant to the Unfair Commercial Practices Directive,[2] the Unfair Contract Terms Directive,[3] the Consumer Rights Directive,[4] the Price Indications Directive[5] (all amended by the Omnibus Directive),[6] the Market Surveillance Regulation,[7] the E-Commerce Directive[8] and voluntary codes of conduct such as the EU Product Safety Pledge (described further below)). Further, to the extent that certain products are illegal or contain harmful information (*e.g.*, books or DVDs), the content is only "spread" to the customers who purchase those products, which is essentially the same for physical retail (book) stores. Therefore, the assumption that the sale of illegal goods on VLOPs could create "systemic risks" is incorrect.

Amazon recognizes that the potential sale of illegal products can negatively impact customer experience in any retail business. Products offered for sale on Amazon must be authentic. The sale of counterfeit products is strictly prohibited. Throughout the selling experience, Amazon's systems monitor selling accounts to identify anomalies or changes in account information, behaviors, and other risk signals. In the event Amazon identifies a risk of fraud or abuse, an investigation is initiated using automated and/or human review, requesting additional information where helpful, and swiftly removing bad actors from the store. As reflected by our strategy and the assessment below, Amazon's focus is on proactively detecting and remediating the causes of the Illegal Content Risk. In 2024, Amazon's proactive controls blocked more than 99% of suspected infringing listings before a brand ever had to find and report them. These listings were suspected of being fraudulent, infringing, counterfeit, non-compliant, or at risk of other forms of abuse.

The sections below describe how the design and functioning of the Amazon EU Store, and the potential misuse of the Amazon EU Store to offer illegal products. Amazon deploys a comprehensive strategy which addresses the Illegal Content risk from a 360 degree-perspective. To prevent illegal content from appearing in its Store, Amazon deploys industry-leading tools to prevent Seller misuse (Section 3.1), ensure brand protection (Section 3.2), guarantee the highest standards of product safety and regulatory compliance (Section 3.3), and ensure trustworthy and reliable reviews (Section 3.4). To mitigate potential risks, Amazon ensures that its advertising and recommender systems are designed to block the amplification of risks (Section 3.5), prevent the reappearance of illegal content (Section 3.6), and ensure that customers are fully refunded for counterfeit or recalled product purchased on the Amazon EU Store (Section 3.7).

[2] Directive 2005/29/EC
[3] Directive 93/13/EEC
[4] Directive 2011/83/EU
[5] Directive 98/6/EC
[6] Directive 2019/2161
[7] Regulation 2019/1020
[8] Directive 2000/31/EC

3.1 Seller verification

Amazon makes it straightforward for businesses to set up a selling account, but very difficult for bad actors to do so.

Amazon verifies the identities of potential sellers through advanced technology and expert human reviewers. Our risk-based algorithmic models and processes for verifying potential Sellers are the first line of defense for our robust proactive controls. Sellers who intend to open a selling account with Amazon must also enter the Amazon Payments – Selling on Amazon User Agreement with Amazon Payments Europe S.C.A. ("**APE**"), and open an account with APE in order to receive payments for online purchases made through the Amazon EU Store, and to transfer funds received for online purchases to a bank account. APE is an Amazon entity incorporated in Luxembourg and licensed as an electronic money institution regulated by the *Commission de Surveillance du Secteur Financier*. APE is subject to strict anti-money laundering obligations, which include verification of the identities and backgrounds of all of its clients. Prospective Sellers are required to provide documents such as government-issued IDs, tax information, business license, phone number, physical address, bank account number, bank routing number, and chargeable credit card. Advanced identity detection methods are employed like document forgery detection, image and video verification, and other technologies to quickly confirm the authenticity of government-issued IDs and whether they match the individual applying to sell in our store. In addition to verifying these, Amazon's systems analyze numerous data points, including behavior signals and connections to previously detected bad actors, to detect and prevent risks. In addition, Amazon has measures in place designed to ensure compliance with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws.

In 2021, Amazon reinforced its Seller verification mechanisms with the introduction of an in-person verification program. This program requires all prospective Sellers to have one-on-one conversations with an Amazon employee to verify the Seller's identity and documentation. Amazon's investigators are trained to verify the authenticity of registration documents and identify common signs of bad-actor behavior, so they can flag high-risk potential Sellers. This process is further enhanced through the verification of the Seller's physical location and payment instruments. Our diligent Seller and product vetting coupled with our efforts to hold bad actors accountable are deterring bad actors from even attempting to enter our store. As an alternative, Amazon introduced instant identity verification processes for prospective sellers in 2024 which significantly decreases the amount of time involved in seller identity verification. This process requires sellers to complete a live video check and demonstrate physical possession of their identification documents.

3.2 Brand protection

Amazon has zero tolerance for counterfeiting and piracy in the Amazon EU Store and is committed to driving counterfeits to zero. Counterfeiting remains a persistent threat around the world. In 2021, the Organization for Economic Cooperation and Development (**OECD**)[9] estimated that pirated and counterfeit products make up 2.5% of world trade — that's $464 billion a year — equal to the

[9] OECD/EUIPO (2025), Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges, Illicit Trade, OECD Publishing, Paris, https://doi.org/10.1787/94d3b29f-en.

gross domestic product of Belgium and, when considering only imports into the EU, these amounted to up to 5.8% of imports. A 2022 Threat Assessment Report carried out by the European Union Intellectual Property Office ("**EUIPO**") and Europol[10] estimated that counterfeit and pirated goods in the EU have an estimated value of up to €117 billion and a more recent 2024 EUIPO study[11] indicates that counterfeit goods cost the clothing, cosmetics and toy industries in the EU €16 billion in sales and nearly 200,000 jobs each year. So, while the prevalence of counterfeits in the Amazon EU Store may be rare, this issue persists through the retail industry and across the globe. The risk of abuse of internet platforms for the sale of counterfeit goods is also identified in public-private partnerships like the Memorandum of understanding on the sale of counterfeit goods on the internet[12] ("**MoU on Counterfeit**"), to which Amazon was a founding signatory since 2011 and is currently part of the working group that is drafting the update to this MOU on Counterfeit. Amazon is a party to similar memorandums of understanding with the German Anti-Counterfeiting Association, the Italian Anti-Counterfeiting Association and the Italian Government in the context of geographical indications acknowledge the risk of counterfeits in e-commerce.

Amazon Brand Protection includes specialist teams who monitor and identify risks related to IP infringement. The tools and processes implemented by Amazon Brand Protection teams are very well-developed and long precede the DSA's entry into force. Each of these teams meets regularly to evaluate key performance metrics, identify trends, align on focus areas, and discuss potential improvements to existing controls through process and tool changes, machine learning, and automation. Brand Protection owns program strategy focused on continuous monitoring to proactively identify and block bad actors from gaining access to Brand Registry (a free service for brand owners empowering brands to manage and protect their brand and IP rights) and related tools, to ensure that Amazon can effectively protect rights owners, Sellers, and customers. This team also deploys catalogue protections to ensure only trusted data is submitted for catalogue listings (each identified by an Amazon Standard Identification Number ("ASIN")), builds products and mechanisms to proactively detect potentially abusive ASINs, and continuously monitors Amazon's catalog to ensure that data does not violate Amazon's IP policy, which prohibits ASINs that infringe others' IP.

Amazon's proactive controls described in Section 3.2.1 blocked more than 99% of suspected infringing listings before a brand ever had to find and report them.

In particular, the number of valid notices of infringement submitted by brands in Brand Registry (described at Section 3.2.2(i) below) has decreased every year since 2020, despite the number of participating brands and the size of the Amazon EU Store catalogue increasing.

---

[10] IP Crime Threat Assessment 2022, https://www.euipo.europa.eu/en/publications/ip-crime-threat-assessment-2022

[11] Economic impact of counterfeiting in the clothing, cosmetics, and toy sectors in the EU, https://www.euipo.europa.eu/en/publications/clothing-cosmetics-and-toy-sectors-in-the-eu-2024

[12] The MOU on Counterfeit states that: "*Even if the vast majority of e-commerce that takes place on the major internet platforms is legitimate, internet platforms can also be abused by some who seek to distribute counterfeit goods. The sale of counterfeit goods over the internet is damaging and harmful to all legitimate stakeholders including internet platforms, intellectual property rights owners and, most importantly, consumers.*" https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en.

Similarly, we have seen a decrease in counterfeits identified by brands participating in the latest MOU on Counterfeit exercise. In fact, fewer than 0.0009% of all products sold on Amazon received a counterfeit complaint from customers. Inspecting the inputs driving counterfeit complaint rates allows Brand Protection to identify root causes driving complaints. In response to information about root causes driving counterfeit complaint rates, Amazon has launched over three thousand additional heuristic rules targeting new infringement abuse use cases. Additionally, in 2024, Amazon identified, seized, and appropriately disposed of more than 15 million counterfeit items, preventing them from harming customers or being resold elsewhere in the retail supply chain.

Amazon's investments in the approach described above contribute to effectively mitigate the risk that infringing products are offered in the Amazon EU Store. The success of Amazon's measures continues to grow over time, and despite the overall growth of the Amazon EU Store, they show that fewer and fewer IP-infringing products are listed on the Amazon EU Store.

More generally, the Amazon EU Store is designed to enable businesses to more efficiently obtain and protect IP rights, which helps brands protect their IP in every store, everywhere, not just on Amazon.

3.2.1 **Robust proactive controls**. In 2017, we launched Amazon Brand Registry, a free service for brand owners regardless of whether they sell in Amazon stores. The service provides brands the ability to better manage and grow their brand with Amazon while protecting their intellectual property rights. Brand Registry allows Amazon to more effectively safeguard brands through automated protections that leverage machine learning and the data provided in Brand Registry. Automated protections use the data brands provide to continuously scan Amazon's store and stop potentially infringing products from being listed.

(i) *Automated IP protections.* Brand Registry allows brand owners with a registered trademark to provide data about their brand, products, and IP. Amazon uses this data to implement predictive protections using advanced machine learning that prevent listings suspected of being infringing. By providing Amazon with information about their IP, brands are enrolled in automated intellectual property protections ("**IPPs**"), also known as automated brand protections, that guard against misuse of their IP on the product detail page. IPPs are implemented based on IP details provided by brands, and operate to scan the catalog for content that appears to infringe the IP, and either remove the ASIN ("*Total ASINs suppressed by IPP*") or listing content ("*Listings enforced by IPP*"). The Increasing number of brands protected by IPP contributes to mitigate the risk that infringing products or listings appear in the EU Store.

(ii) *Catalog authorization protections.* Amazon enrolls brands in a suite of protective tools called "catalog authorization protections". These are protections that restrict the creation and editing of branded listings to the rights owner, Amazon, or other qualified contributors (e.g., Sellers with lengthy or defect-free sales history of branded items). As brand rights owners are the most trusted sources of information about their own products, increasing the coverage of catalog authorization protections mitigates the risk that infringing products or listing content appears in the Amazon EU Store.

(iii) *Closed feedback loop*. Amazon's automated technology scans billions of attempted changes to product detail pages daily for signs of potential abuse, including the creation of new listings and changes to existing listings. For example, our tools use advanced machine learning to prevent the attempted listing of counterfeit or infringing products scanning keywords, text, and logos which are identical or similar to registered trademarks or copyrighted work. We use the data and learnings gathered throughout these processes to innovate and improve our proactive protections. When we receive a valid notice of infringement or a customer complaint, our machine learning algorithms use this information to learn and improve protections for brands. When the tools detect a possible issue, the listing may be blocked from publication, removed, or required to undergo a further detailed review by expert investigators to confirm whether it is infringing. If content is confirmed to be infringing, Amazon removes it from the Amazon EU Store.

Amazon monitors the number of repeat suspended Sellers, i.e., Sellers that have been suspended for policy violations and reinstated following a Seller appeal, and which are subsequently suspended again as a result of IP infringement or abuse. Learnings from tracking these repeat suspended Sellers help us identify abusive behavioral patterns and inform improvements in upstream Seller account suspensions.

3.2.2 **Powerful tools to protect brands.** Amazon offers a number of services through the Amazon EU Store to support brands in securing and protecting their IP rights.

(i) *Brand Registry*. In addition to facilitating the proactive controls described above, within Brand Registry brands can leverage the Report a Violation tool to search for, identify, and report infringements using image and text search technology. The report on the functioning of the MOU on Counterfeit recognizes that these notification tools are "*indispensable measures in the fights against the sale of counterfeit goods*." Brands also receive more control over the photos, videos, text, and other information on product detail pages associated with their brand, so they can ensure their product information is accurate and help customers make confident, informed purchasing decisions.

As said above, the number of valid notices of infringement decreases year on year. The [Confidential] owns a goal to reduce this number and tracks relevant metrics. [Confidential] This is due, among other things, to the enhanced operation of Amazon's proactive controls.

(ii) *Amazon IP Accelerator*. Amazon's IP Accelerator[13] service connects businesses in Europe with a curated network of trusted IP law firms, which provide high-quality trademark registration services in 18 languages at competitive rates. These businesses can also register for Brand Registry, even with a pending trademark, allowing them to utilize and benefit from Amazon's tools to protect their brand.

[13] https://brandservices.amazon.com.be/ipaccelerator

(iii) *Project Zero*. Amazon also offers Project Zero,[14] a self-service counterfeit removal tool empowering brands to act as trusted flaggers and remove counterfeit products themselves from the Amazon EU Store. If Amazon's solutions somehow miss a counterfeit product, eligible brands have the power to directly remove a counterfeit product from the Amazon EU Store in near real-time without the need to contact Amazon. Brands can quality for Project Zero regardless of their selling relationship with Amazon if they have submitted reports of potential infringements through Brand Registry with an acceptance rate of at least 90% over the previous six months.

(iv) *Transparency*. Transparency is Amazon's product serialization service that prevents counterfeits from reaching customers by using codes to uniquely identify individual units of enrolled products. These codes can be scanned throughout the supply chain and by customers to verify authenticity, regardless of where the products were purchased (*i.e.*, on Amazon or elsewhere). More than 2.5 billion product units have been verified as genuine through Amazon's Transparency program. Transparency is also interoperable with brands' existing serialization systems - allowing brands to enroll without requiring any changes to their manufacturing or packaging processes. Over 88,000 brands use Transparency, including Fortune 500 companies, global brands, startups, and small businesses.

3.2.3 **Holding bad actors accountable**. Amazon is committed to working together across the private and public sectors to stop counterfeiters. In partnership with brands and law enforcement, we have been able to hold more bad actors accountable through civil litigation and criminal referrals to law enforcement organizations—working to stop them from abusing our and other retailers' stores across the industry in the future. Our collaborative approach enables rapid exchange of intelligence with customs officials, police authorities, and rights holders across multiple countries. These partnerships have led to significant enforcement actions, including the joint development of new strategies to identify and stop bad actors at the source. In 2024, Amazon's cross-border work with law enforcement led to more than 60 successful raid actions, with over 100 bad actors identified and detained. When we find a counterfeit, we go beyond the Amazon EU Store. We go upstream to identify the warehouses and distribution network involved in counterfeit production so we can prevent the counterfeit products from re-entering the supply chain. This protects and benefits customers whether they are shopping on Amazon or elsewhere

(i) *Enforcement of terms and conditions.* If our tools identify potentially infringing content, the listing may be blocked from publication, removed, or required to undergo a detailed review by expert investigators. If an issue with the listing or product is confirmed, Amazon protects customers and brands by blocking the listing from publication, removing the problematic content or listing, blocking accounts and/or referring bad actors to law enforcement.

(ii) *Disrupting counterfeit networks across the globe.* Misusing the Amazon EU Store to offer an inauthentic product can also constitute a criminal offence. In order to increase

[14] https://brandservices.amazon.com.be/projectzero

litigation efforts and collaboration with law enforcement around the world, the Amazon Counterfeit Crime Unit ("**CCU**") was established in 2020.

Amazon's CCU is a global team that includes former law enforcement investigators and prosecutors, and data analysts. Amazon's CCU pursues civil suits and works with law enforcement on joint enforcement and seizures across the globe, including taking action against bad actors, suppliers, logistics providers, social media influencers, fake invoice providers, and more. In partnership with brands and law enforcement, we have been able to hold more counterfeiters accountable stopping them from abusing our and other retailers' stores across the industry. Amazon's CCU has taken strong enforcement action (in and out of court) against pan-European counterfeit networks, including companies and individuals, that defraud customers and harm the reputation of brand owners and Amazon by selling counterfeit products in the Amazon EU Store.

These efforts have yielded concrete successes, including filings, both civil and criminal, as well as investigative and legal results during the relevant period:

- Amazon and Brother jointly filed a civil action in Germany against a network of 18 bad actors selling counterfeit Brother toner cartridges in the Amazon store. In July 2025, a German court issued a judgment, ruling entirely in favor of Amazon and Brother. All 18 defendants were held liable, some of them through default judgments, others, who had filed a defense and contested the claims, after a full evidentiary review. The judgment confirms Amazon's and Brother's right to damages, orders the destruction of counterfeit goods, and mandates supply chain disclosure. It also acknowledges the defendants' coordinated behavior as a counterfeiting network.

- In July 2024, a major anti-counterfeiting operation led by UK customs officials in collaboration with CCU, LEGO, and Chinese law enforcement resulted in one of the largest seizures of counterfeit toys to date. The investigation was triggered when customs officials identified a Chinese bad actor attempting to distribute counterfeit products through 15 different bad actor selling accounts in Amazon's UK store. Following CCU's initial probe and subsequent collaboration with LEGO's IP legal teams in Europe and China, local law enforcement uncovered an extensive counterfeiting network in southern China, including live streamers, sellers, wholesalers, and manufacturing facilities. The successful multi-site raid led to the detention of 45 suspects and the seizure of over 60,000 copycats and 390 infringing moulds used in their production.

3.2.4 **External engagement and education**. Amazon actively engages to collect external input on our brand protection tools, including through managed relationships with Sellers and brand owners. Amazon also invests to educate Sellers on opportunities to protect their IP and ensure they offer authentic and non-infringing products and protect customers with information on how to shop confidently and avoid counterfeit products.

(i) *Engaging externally*. Amazon regularly consults with brand owners through managed relationships and organized forums. These external engagements help inform Amazon's understanding of the concerns of brand owners and their feedback based on use of Amazon's brand protection tools. The learnings from these relationships allow Amazon to identify particular pain points and emerging risks, and cooperation with brands enables Amazon to refine existing controls. For example, to solve the issue of bad actors identified as repeat infringers who pass through product authenticity reviews using falsified documentation (*e.g.*, forged receipts or brand authorization letters), Amazon collaborated with brands to create an enhanced supply chain verification process. We learned that bad actors are savvy enough to create legitimate looking invoices complete with logos, real addresses, product names, and can even be made to look like it has been signed by an attorney matching the one named on record on a trademark certificate. The enhanced verification process identifies brand-specific indicators of inauthentic invoices and letters of authorization.

(ii) *Educating Sellers.* Amazon EU Store's Intellectual Property Policy[15] provides clear and practical information to Sellers about IP rights and common IP concerns that might arise when selling on Amazon, including regarding the enforcement of those rights.

(iii)*Protecting and educating customers*. We make available materials that help raise customer awareness about counterfeit products to promote purchases of authentic products. For example, we organized an event for over 600 students of H-FARM College, called 'Challenge the Fake' with INDICAM, the Italian association for the protection of intellectual property. The students were asked to suggest concepts for communication and marketing campaigns targeting their peers in order to tackle the sale of counterfeit items and promote the protection of intellectual property. In collaboration with the International Trademark Association (INTA), Amazon launched the 2024 Unreal Campaign Challenge, asking global DECA members to produce a 60-second public service announcement video that highlights the dangers of purchasing counterfeit. The winners were recognized at DECA's annual International Career Development Conference (ICDC) in front of thousands of students. In support of INTA's Unreal Campaign, Amazon also gave a lecture to MBA students at the SDA Bocconi campus in Milan, raising awareness about counterfeiting and the importance of partnership. In 2024, Amazon and Andema (Spanish Association for the Defense of Brands), hosted the third annual Brand Protection Day event in Madrid. The event was open to Andema's members, consisting of numerous Spanish brand owners and company executives.

(iv)*Establishing strategic partnerships*. Amazon has a memorandum of understanding in place with the Italian Ministry of Internal Affairs that aims to bolster the fight against counterfeiters in Italy. Via the MOU, Amazon shares information about identified counterfeiters' modus operandi with the Ministry, supporting their internal efforts to develop policies and resources that support law enforcement action. With this

[15] Amazon Intellectual Property Policy, https://sellercentral.amazon.de/help/hub/reference/external/G201361070?locale=en-US.

partnership, Amazon and the Ministry have highlighted the importance of collaboration and prioritizing anti-counterfeiting resources for law enforcement.

In 2024, Amazon established a formal partnership with the EUIPO, as part of a Call for Expression of Interest put forth by the EUIPO. This will allow both entities to publicly collaborate on marketing initiatives focused on raising awareness about IP and Brand Protection. The partnership builds on Amazon's longstanding engagement with the EUIPO. In 2023, Amazon joined the EUIPO Intellectual Property Enforcement Portal (IPEP) as both a business and a rights owner. IPEP is a centralized platform for the exchange of information related to IP rights and includes customs officials, police authorities, rights holders, and now marketplace service providers, who are dedicated to identifying and stopping counterfeits from reaching consumers. This collaboration will enhance Amazon's existing efforts and extend our reach to brands currently not on Amazon, underscoring our commitment to combat counterfeit.

Together, these performance metrics show that the measures Amazon employs to guard against the risk of IP-infringing products are effective, robust and far-reaching.

3.3 Product safety and compliance

Amazon has always sought to be the Earth's most customer-centric company, therefore we strive to ensure that only safe and compliant products are offered in the Amazon EU Store. Exposing our customers to illegal or unsafe products would be wholly contrary to our customer-centric business model.

Amazon demonstrated its commitment to better product safety in Europe as a founding signatory to the 2018 EU Product Safety Pledge, and reconfirmed that commitment by signing the Product Safety Pledge + in 2023. Amazon recognizes that all retailers must remain vigilant on product safety, as evidenced by the 4137 alerts of dangerous non-food products notified to Safety Gate in 2024[16]. All products offered in the Amazon EU Store must comply with applicable laws, including product safety and compliance requirements. Compliance with these laws starts with our Sellers, and the design and function of the Amazon EU Store contributes to their ability to offer a safe and compliant customer experience. Amazon's investments in the four strategic pillars described above contribute to the ability to effectively mitigate the risk that unsafe or non-compliant products are offered in the Amazon EU Store.

Amazon deploys a suite of powerful tools to continuously monitor and proactively remove non-compliant products from our EU Store, using both automated and expert human reviews. These tools are implemented by our Regulatory Intelligence, Safety, and Compliance ("**RISC**") team, which is responsible for protecting customers from products that are unsafe, illegal, illegally marketed, controversial, or otherwise violating Amazon's safety and compliance policies. It does this by: (i) proactively collecting information from Sellers to determine whether their product should be allowed for sale in the EU Store, (ii) educating Sellers about their compliance obligations and validating information provided by Sellers; (iii) identifying risks and implementing controls across the EU Store, covering products such as food, toys and chemicals (among others) to identify

[16] https://ec.europa.eu/safety-gate/#/screen/pages/reports

potentially non-compliant ASINs; (iv) removing ASINs identified as non-compliant or unsafe; (v) informing customers who have purchased unsafe products in a timely manner and (vi) engaging with regulators, both proactively to inform their understanding of Amazon's product safety and compliance programs, and reactively when non-compliant ASINs are identified.

RISC is made up of specialist teams that anticipate, identify and monitor the risks related to product safety and compliance, and design and enforce mitigation measures. These teams meet periodically to evaluate key performance metrics, surface emerging product safety and compliance risks (external and internal to Amazon), and discuss and align on potential issues.

RISC is also responsible for designing, building and operating Seller enforcement and education programs and seeks to reduce customer exposure to prohibited, regulated, and restricted products by increasing Seller compliance, and prevent or remove bad actors that attempt to offer non-compliant products on Amazon. RISC identifies Sellers that repeatedly violate the same policy or multiple policies over a period of time.

The metrics tracked by the RISC team demonstrate that the Amazon EU Store is getting safer overall, and they allow for constant improvement of Amazon's controls:

- [Confidential]
- [Confidential]

3.3.1 **Robust proactive controls**. The Amazon EU Store's content moderation systems aimed at product compliance include proactive listing controls that function through automated rules ("**Product Listing Rules**") to identify and remove non-compliant products. Product Listing Rules include (i) more than ten thousand safety and compliance keyword-based algorithms which take into account the localized nature of product compliance requirements and linguistic differences of each of the Storefronts consistent with Article 34(2) of the DSA, and (ii) a variety of machine-learning models continuously running against the Amazon EU Store's catalogue of product offers. These models analyze data points related to the products, brands, offers and Sellers, to detect activity that indicates certain product offers might violate Amazon's policies.

New information, including internal learnings and developments and external risk signals, is fed into our tools daily so they can learn and continually get better at proactively identifying and blocking non-compliant products. These Product Listing Rules prevent [Confidential]. As of August 2025, Amazon proactively stopped over 111 million products in the EU for safety or compliance reasons. Nearly all of those proactive suppressions occurred before a single item was sold. Specific applications of the Product Listing Rules in moderating content in the Amazon EU Store are described further below.

(i) *Products that may not be sold in the Amazon EU Store.* Certain products, such as firearms, cigarettes, or illegal drugs, may not be sold in the Amazon EU Store either because they are illegal or violate our policies. Amazon implements Product Listing Rules that prevent any Seller from listing these products.

(ii) *Products that may be sold in the Amazon EU Store if additional information is provided*. Certain products may be sold in the Amazon EU Store only under certain conditions. Amazon is able to identify these products based on internal and external risk signals. For example, recently Amazon became aware of an increased risk with solar eclipse glasses and climbing harnesses. Therefore, Sellers of these products must show that their products meet the specific compliance and/or safety criteria that address the product-specific risks. To that end, Sellers must provide Amazon with the information necessary to confirm that the products are safe and comply with legal requirements, like EU Declarations of Conformity, proof of *Conformité Européene* ("**CE**") markings, Global Food Safety Initiative certificates and evidence of notification to relevant authorities, or test reports from independent accredited laboratories illustrating compliance to harmonized European Standards.[17] If Sellers do not provide this information, the listing is no longer allowed in the Amazon EU Store

(iii)*Products that may only be sold in the Amazon EU Store by qualified Sellers*. Certain products may only be sold by qualified Sellers. For these types of products, Amazon

[17] *See*, for example, the relevant requirements for Personal Electronic Mobility (E-mobility) Devices, https://sellercentral.amazon.com.be/help/hub/reference/external/G201978810?locale=en-US, and Fidget Spinners, https://sellercentral.amazon.de/help/hub/reference/external/202155900?ref=efph_202155900_relt_4QUDFLRX8GBFPVV&locale=en-US

verifies whether the Seller has the necessary qualifications and authorizations, *e.g.*, whether the Seller who wants to sell certain human medicines is a pharmacy and has a license to sell medicines online.[18] For other products that require Seller licenses or restrictions and we have assessed that our systems do not support Seller compliance or they present a customer safety risk, such as prescription medicines or explosive precursors listed in Annex I of the Explosive Precursor Regulation,[19] we prohibit these products through our policies and Product Listing Rules.

3.3.2 **Powerful tools to support product safety**. We make a suite of powerful tools available for Sellers to ensure their products are offered in accordance with applicable law.

(i) *Manage Your Compliance*. The Amazon EU Store offers several tools and systems to empower and facilitate Sellers' compliance. Through an interface called "Manage Your Compliance", Sellers are prompted to provide relevant product safety and compliance materials, including product compliance warnings and markings on product pages and high-quality 6-sided images of their products and packaging. Often and where available, we leverage APIs to public resources to help make compliance easy and reliable. For example, Sellers can display energy efficiency labelling by simply giving us their European Product Registry for Energy Labelling ("**EPREL**") ID information.

(ii) *Compliance solutions*. In addition, Amazon provides compliance solutions[20] to help Sellers meet and manage their compliance obligations, including extended producer responsibility[21] and responsible person services.[22] We also connect Sellers with third-party service providers to manage their compliance obligations by suggesting service providers for testing, labelling and other compliance needs, often at pre-negotiated discounted rates.[23]

(iii) *Dedicated point of contact*. Occasionally, Amazon is notified of a product listing that is unsafe or may violate applicable laws or Amazon's policies. Regulators can contact us directly via a dedicated alias to inform us of an unsafe or non-compliant product for takedown. When we receive a notice from an authority, we act quickly to protect customers, remove unsafe products from the Amazon EU Store, and investigate.

---

[18] *See*, for example, the relevant requirements for Drug, Drug Paraphernalia and Dietary Supplements, https://sellercentral.amazon.de/help/hub/reference/external/G201743990?locale=en-US

[19] Regulation (EU) 2019/1148

[20] Amazon Compliance Solutions, https://sell.amazon.de/einhaltungs-losungen?ref_=sdde_soa_cs_n

[21] Amazon Compliance Solutions, Environmental Security, https://sell.amazon.de/en/einhaltungs-losungen/umweltshicherheit. These services help Sellers manage their extended producer responsibility (EPR) requirements (for example, registration of products, reporting of waste, payment of eco-contributions and take-back obligations) under applicable law.

[22] Amazon Compliance Solutions, Product compliance, https://sell.amazon.fr/en/solutions-conformite/produit. These services are available to Sellers that are based outside the EU and use FBA and allow them to comply with the requirement under the Market Surveillance Regulation to appoint a Responsible Person based within the EU for CE-marked products.

[23] Amazon Service Provider Network, https://sellercentral.amazon.com/gspn?&ref_=xx_gspn_servs_hp#/search/EU/compliance?product_category=product_hardlines_electronics&localeS election=en_US

(iv) *Product recalls*. We actively monitor public recall notifications by checking Safety Gate twice daily and monitoring 50 recall sites for the EU. For recalled products, we have built systems not only to remove and prevent future product listings but also to directly inform past customers (unlike most physical-store retailers) to ensure that they stop using the product. Customers are able to visit a section of their Amazon account dedicated to informing them about recalled products. We also give customers the option to opt in to receive push notifications on their mobile devices. Customers are notified with a banner if one of their products is affected by a recall. Amazon can use this information to expand, refine, and improve its proactive Product Listing Rules.

In Q1-Q2 2025 we removed 613,295 unsafe ASINs due to public recalls. In Q1 and Q2 2025, we removed over 10,455 ASINs that our safety investigations confirmed were potentially unsafe products or for which we were missing information, although our ability to identify recalled products relies on the quality and completeness of the public recall notice. Public recall data helps us to identify product safety trends and consider potential enhancements to our controls through Product Listing Rules.

3.3.3 **Holding bad actors accountable**. Amazon shares with law enforcement agencies across Europe potential suspicious customer transactions and their relevant data points, such as customer information in accordance with the Explosive Precursor Regulation.[24] For this purpose, Amazon has appropriate, reasonable and proportionate measures in place to control transactions and investing enormous efforts into identifying and reporting transactions that may be suspicious when combined with information that law enforcement may have. Amazon has classified several hundred thousand products for which transactions are monitored and complex combination purchases are flagged for potentially being suspicious. All of the results are reviewed by risk managers, to ensure correct reporting considering the impact an incorrect report might have on our customers and on the general public. Our efforts in working with the authorities and law enforcement agencies is underlined by the fact that we are actively participating in the EU Standing Committee on Precursors, the German "Arbeitskreis on Explosive Precursors" and are in close contact with the relevant national contact points. In light of this participation we have contributed to the Guidance Documents released by the Commission on the identification and reporting of suspicious precursors.

3.3.4 **External engagement and education**.

(i) *External engagement.* As memorialized in the Product Safety Pledges, Amazon is committed to close cooperation with the Commission and other authorities.

(ii) *Seller education*. Amazon recognizes that most Sellers share Amazon's mission to protect consumers, contributing to Amazon's goal to provide the world's largest selection of safe and authentic products, but Sellers may unknowingly list a non-compliant or prohibited product because they are unaware of an applicable legal requirement or Amazon policy. When we identify and remove a non-compliant or unsafe product offer, we inform the Seller of the violation and provide additional

[24] Regulation (EU) 2019/1148

information about Amazon's policies and compliance resources to help them be compliant on their own in the future.

completeness of the public recall notice. Public recall data helps us to identify product safety trends and consider potential enhancements to our controls through Product Listing Rules.

3.3.5 **Holding bad actors accountable**. Amazon shares with law enforcement agencies across Europe potential suspicious customer transactions and their relevant data points, such as customer information in accordance with the Explosive Precursor Regulation.[25] For this purpose, Amazon has appropriate, reasonable and proportionate measures in place to control transactions and investing enormous efforts into identifying and reporting transactions that may be suspicious when combined with information that law enforcement may have. Amazon has classified several hundred thousand products for which transactions are monitored and complex combination purchases are flagged for potentially being suspicious. All of the results are reviewed by risk managers, to ensure correct reporting considering the impact an incorrect report might have on our customers and on the general public. Our efforts in working with the authorities and law enforcement agencies is underlined by the fact that we are actively participating in the EU Standing Committee on Precursors, the German "Arbeitskreis on Explosive Precursors" and are in close contact with the relevant national contact points. In light of this participation we have contributed to the Guidance Documents released by the Commission on the identification and reporting of suspicious precursors.

3.3.6 **External engagement and education**.

(i) *External engagement.* As memorialized in the Product Safety Pledges, Amazon is committed to close cooperation with the Commission and other authorities.

(ii) *Seller education*. Amazon recognizes that most Sellers share Amazon's mission to protect consumers, contributing to Amazon's goal to provide the world's largest selection of safe and authentic products, but Sellers may unknowingly list a non-compliant or prohibited product because they are unaware of an applicable legal requirement or Amazon policy. When we identify and remove a non-compliant or unsafe product offer, we inform the Seller of the violation and provide additional information about Amazon's policies and compliance resources to help them be compliant on their own in the future.

[25] Regulation (EU) 2019/1148

3.4 Trustworthy customer reviews

Having authentic and trustworthy reviews is essential for the reputation and credibility of the Amazon EU Store[26], while inauthentic or misleading reviews harm customers' trust[27] and lead to erosion of the Amazon brand and lower sales over time.

Amazon introduced customer reviews in 1995 with the purpose of providing authentic customer insights about products and services offered in its store and enabling customers to make better informed purchasing decisions. Every year tens of millions of customers contributed one or more product reviews or ratings to Amazon's EU Store, providing Amazon customers with transparent insights into the products they were considering. Since 1995, we have continued to innovate on review features that help shoppers easily see and share positive and negative customer feedback that is relevant, helpful, and trustworthy.

Our goal is to ensure that every review in the Amazon EU Store is trustworthy and reflects customers' actual experiences. For that reason, Amazon welcomes authentic reviews — whether positive or negative — but strictly prohibits[28] fake reviews that intentionally mislead customers by providing information that is not impartial, authentic, or intended for that product or service ("**Fake Reviews**"). Amazon encourages the pluralism of opinions that benefit our customers and only moderates customer reviews content if the review would either violate Amazon's policies or applicable laws. Consistent with its strategy to protect customers from all forms of abuse, Amazon has implemented effective countermeasures to prevent misleading customer reviews from appearing in the Amazon EU Store. As a result of continued investments, Amazon proactively blocked over 275 million suspected Fake Reviews from our stores in 2024.

Fake Reviews include any reviews that are created, edited, or removed in exchange for compensation, and any review where the intention is to provide a view which does not reflect the customer's actual experience with the product. Compensation can be via direct payment, but also includes indirect compensation via discounts, free products, gift cards, and refunds. Bad actors engage in Fake Reviews in different ways including by: employing companies or individuals directly to create fake or incentivized reviews; creating multiple fake accounts, including personal accounts, for positive review of their own products or abusive reviews of their competitors' products; taking over or compromising customer accounts to submit false reviews; and using review brokers to source reviews in order to artificially make their products look more attractive. As this misconduct is often orchestrated outside of Amazon's EU Store, it can be more challenging to detect, prevent, and enforce these bad actors if we are acting alone. Amazon therefore gathers

[26] Creating a Trustworthy Reviews experience, https://www.aboutamazon.com/news/how-amazon-works/creating-a-trustworthy-reviews-experience

[27] European Parliament 2015 briefing, Online consumer reviews: The case of misleading or fake reviews, https://www.eesc.europa.eu/sites/default/files/resources/docs/online-consumer-reviews---the-case-of-misleading-or-fake-reviews.pdf

[28] Customer Reviews, https://www.amazon.de/-/en/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=G3UA5WC5S5UUKB5G

information on the risk of Fake Reviews through proactive review of both the EU Store and third-party sites, and user reports.

As set out in more detail below, a specialized team within Amazon works on curbing Fake Reviews, and assesses performance metrics to identify action items on a weekly basis. It also meets for quarterly business reviews to discuss general trends and identify areas of improvement. Their operational plan for the year is continuously refined and also includes initiatives aimed at improving the customer trust experience for reviews. The key performance metrics monitored by this team include auditing of the number of products that are associated with Fake Reviews, customer trust perception in Amazon's reviews, and social media groups that engage in abuse.

3.4.1 <u>Robust proactive controls</u>.

(i) *Proactive review of the Amazon EU Store*. Amazon invests significant resources to proactively review the Amazon EU Store to detect the risk of Fake Reviews. We use proactive controls to detect and remove Fake Reviews, including machine learning models that analyze millions of reviews each week using thousands of data points to detect risk related to, for example, links to other accounts, sign-in activity, review history, and other indications of unusual behavior. In addition, expert investigators use sophisticated fraud-detection tools to analyze and prevent Fake Reviews from ever appearing in the Amazon EU Store. Amazon's fraud-detection tools are designed to identify fake and incentivized reviews, which occur in different forms that have evolved over time. [Confidential]

Initially, bad actors used to create fake customer accounts with the purpose to post Fake Reviews; bad actors then moved to including review solicitations in product packages (*i.e.,* product inserts) asking customers to leave 5-star ratings in exchange for a free product or rebate; and more recently reviews brokers started soliciting positive reviews directly from customers in return for some form of compensation like a gift card or free product.

To identify bad actors, Amazon [Confidential]

Amazon's Fake Review detection tools are constantly inspected to identify opportunities for further refinement. For example, [Confidential]

(ii) *Proactive review of third-party sites.* The transactions underlying Fake Reviews usually take place outside the Amazon EU Store. Amazon therefore reviews third-party sites to identify potential forums for soliciting or requesting Fake Reviews.

We monitor social media sites to identify abusive Seller accounts that use social media to violate Amazon's policies by offering compensation in exchange for reviews. We have a team of investigators that continuously monitor and search social media sites for terms like: "Amazon Free", "Amazon gift card" etc. across groups, marketplaces, posts and tweets. We then use the respective social media website's reporting function to report these on a weekly basis. We only report groups that we have very high confidence are abusive. Because these groups are the source of Fake Reviews, it is important that our takedown requests are actioned and that this occurs

expeditiously. For this reason, we also track whether the social media company took down the groups that we reported. We have continued to work with these companies, including escalating to senior executives when necessary to improve their takedown accuracy. In 2024, we have reported over 1.5 million abusive pages, post and groups across social media websites and successfully removed 910,149 abusive pages, post and groups across social media websites.

We have also collaborated with social media platforms [Confidential].

(iii) In 2024 we reported to social media companies more than 15,166 groups that facilitated Fake Reviews on social media sites. We believe our efforts to educate social media users and action these groups more quickly have deterred bad actors from pursuing Fake Reviews, leading to a year-over-year reduction in the number of groups we've identified and reported.

(iv) *User reports*. We measure our customer's perception of trust in product reviews through customer surveys on a weekly basis across Germany, France, Italy and Spain. The survey is conducted blind, meaning participants do not know Amazon is conducting the study. We then use monthly and quarterly insights from this survey to prioritize work across multiple Amazon teams. [Confidential]

3.4.2 **Powerful tools to support trustworthy reviews**. The review ranking algorithm that allows customers to read "Top reviews" considers signals from Amazon's fraud-detection tools based on the authenticity of a review. When the signal is strong (*i.e.*, we strongly suspect that the review is inauthentic), we suppress the review completely, so it is not displayed in the Amazon EU Store. When the signal is moderate (*i.e.*, we suspect it may be inauthentic but still need to gather additional data points), the reviews are down-ranked to the bottom of the list until we can verify their authenticity. Customers can also report abusive customer reviews directly to us through the "Report Abuse" tool available next to each review. We review and process every complaint we receive using machine learning models, expert investigators, and content moderation processes, and take corresponding actions against inauthentic reviews. We also use learnings to enhance our machine learning models and moderation processes.

3.4.3 **Holding bad actors accountable**. As our countermeasures have become more effective, the tactics of bad actors have also evolved in an attempt to try to evade detection. Most recently an illicit industry has developed with Fake Reviews brokers looking to profit by offering, procuring, selling, or hosting public and private groups on third party sites where Fake Reviews are exchanged for compensation. These brokers approach consumers directly through websites, social media channels, and encrypted messaging services, soliciting them to write Fake Reviews in exchange for money, free products, or other incentives.

In cases where we uncover evidence of review abuse, we take swift and decisive enforcement action against the offending Seller or reviewer, not only to remove the abusive content or perpetrator from the Amazon EU Store but also to address the underlying cause, including through litigation. Amazon provides Sellers and reviewers with a robust

complaints process to remedy any potential errors in its investigation and enforcement process. As we understand that violations can occur due to a lack of customer awareness, we adopt measures to improve customer awareness.

Amazon also adopts a global approach of enforcement action (in and out of court) against companies and individuals that facilitate misleading reviews, as these bad actors often solicit reviews across geographies. By taking such action, Amazon targets the source of the problem. These efforts have yielded concrete successes for our Amazon EU Stores:

- In May 2025, Amazon and TripAdvisor jointly filed a civil action before the Milan court against a group of fake review brokers operating under the "Pagini brothers" network. The defendants ran multiple sites — including comprarerecensioni.it and marketing-seo.it — selling fake reviews to Italian businesses. Both Amazon and TripAdvisor are members of the Coalition for Trusted Reviews, and the case aligns with joint efforts to strengthen review integrity in Europe.

- In June 2025 several France-based websites advertising fake reviews services were formally referred to the French regulator DGCCRF. In parallel, CCU issued several C&D letters to operators of fake review brokers websites, leading to takedowns of five targets.

- In January 2024, Amazon won a key battle against Fake Reviews in Italy, following a ruling issued by the Court of Milan against a bad actor who attempted to facilitate the posting of 5-star ratings on the Amazon.it Store. The ruling led to the immediate closure of the Italian Fake Review website, Realreviews.it, and prohibited its operator from conducting similar activities in the future. The Milan court ruling came in response to legal action taken by Amazon against Realreviews.it, which revealed how the site offered prospective reviewers a full refund for purchased products if they published and provided proof of a 5-star review. The court ruled that the website's owner acted in violation of unfair competition laws, thereby causing harm to both Amazon and its customers. This legal action in Italy was part of a wider ongoing campaign by Amazon to stop Fake Reviews globally.

- Also in 2024, in March, Amazon achieved a new success in its fight against Fake Reviews in Spain in coordination with a local major consumer organization. After taking appropriate legal action, a fraudulent scheme that encouraged the publication of fake 5-star reviews in the Amazon.es Store was shutdown. In this case, Amazon filed a civil lawsuit against the administrators of a group that promoted Fake Reviews from Spain using the encrypted messaging application Telegram to carry out such fraudulent actions. The group in question operated under the name of "Productos Gratis".

Amazon not only takes action against Fake Review brokers, but our actions are directed against anyone who participates in this illegal business.

- In September 2023 Amazon obtained a decision against a major German Fake Review broker before the Cologne Higher Regional Court. In the underlying proceedings, Amazon sought injunctive relief and information against e-tailbooster GmbH and its

managing director. In the first instance, the Cologne Regional Court issued a default judgment (November 2022) against e-tailbooster and its director granting the claim for information in full, i.e. including information on the Sellers who purchased Fake Reviews. The default judgment was then confirmed by the Cologne Regional Court following an appeal. In the subsequent appeal proceedings, the Cologne Higher Regional Court accepted Amazon's arguments and has now also largely confirmed the judgment. This means that Amazon has for the first time obtained a judgment confirmed by a German higher court, which entitles Amazon to information about the reviews sold and the customers of a review broker.

- Amazon regularly enforces the judgments and injunctions obtained against Fake Review brokers and applies for penalties in case of non-compliance. For example, Amazon filed two fine applications against German Fake Review brokers (ShopDoc GmbH and Martin von der Hocht). In mid-August 2023, the Hamburg Regional Court imposed a fine of EUR 10,000 on Vorwärts GmbH and its director because they had not complied with the Court's judgement and had not provided information on the reviews that Vorwärts GmbH had sold. Amazon is currently enforcing this fine against Vorwärts GmbH. In 2024, the Hamburg Regional Court also imposed a fine against Martin von der Hocht. Amazon also filed a fine application against the German Fake Review broker ShopDoc GmbH at the end of 2023. Furthermore, the Hamburg Regional Court (confirmed by the Higher Regional Court) imposed imprisonment of one full week against a review broker.

- To improve its Fake Review countermeasures, Amazon regularly files actions against Fake Review brokers to obtain information about the relevant Sellers. In addition, Fake Review brokers regularly undertake to provide Amazon with detailed information about their review business as part of settlement agreements.

3.4.4 External engagement and education.

Amazon remains committed to holding bad actors accountable to protect our customers and Sellers. Fake Review brokers represent a global challenge, impacting customer reviews across multiple industry sectors. Addressing this issue effectively requires collaborative efforts from the private sector, consumer groups, and governments to target the root cause and clearly communicate that such illicit activities must cease.

To this end, Amazon has introduced a Fake Reviews Blueprint, advocating for private and public sector partnerships. This initiative promotes: (a) enhanced information sharing about known bad actors, their tactics, targets, services, and operational methods, (b) clearer enforcement authority and increased funding to hold bad actors accountable, and (c) improved controls for services that facilitate Fake Review solicitation.

Amazon also co-founded the Coalition for Trusted Reviews, a cross-industry collaboration dedicated to safeguarding access to trustworthy consumer reviews. The coalition's inaugural conference, hosted by Amazon, aimed to establish the organization as a respected convener of thought leaders and influential stakeholders in the realm of trustworthy online reviews, while showcasing Amazon's role as a trusted partner and leader in combating fake reviews. The event included a public segment, uniting government officials, consumer groups,

industry associations, and non-coalition members to raise awareness about the issue of Fake Reviews.

While our collaborative efforts with third-party services have yielded improvements in response times to takedown requests from some service providers, we advocate for robust, effective, and swift notice and takedown processes across all platforms that could potentially facilitate illicit activities. To disrupt Fake Review networks and address the problem at scale, we seek to collaborate with third parties to enhance their detection methods and implement stronger controls for proactively identifying and shutting down these networks. Furthermore, we believe that through joint efforts, we can better educate customers about Fake Review solicitation and ensure rigorous enforcement policies for Fake Review brokers.

3.5 Advertising and recommender systems in the Amazon EU Store

Amazon's overall strategy in protecting the Amazon EU Store from all forms of abuse seeks to prevent illegal, inauthentic, and infringing products from being listed in the Amazon EU Store in the first place. The risk of infringing, inauthentic, non-compliant, and unsafe products being amplified to a large number of users of the Amazon EU Store via advertisements or the design of recommender systems is low because of our efforts to prevent those products from being sold in the Amazon EU Store at all. Further, the design of advertising and recommender systems in the Amazon EU Store contributes to mitigate the potential amplification of risks impacting the Systemic Risk Categories.

The DSA stresses the "systemic" nature of the risks due to potential amplification of illegal and harmful content through online platforms. Online marketplaces do not amplify this information like purely digital players that function as de facto "public spaces" in the online world. The purpose of customer's visit to the Amazon EU Store is to consider a purchase, not consume scrollable content. Consequently, to the extent that certain goods contain political information, or information with relevance to democratic process (e.g., books or dvds), such content is only "spread" to the customers who purchase such products. This is essentially the same risk for physical retail stores and cannot be described as a risk that is systemic in nature. The advertising and recommender systems in the Amazon EU Store do not contribute to that risk.

3.5.1 Advertising in the Amazon EU Store

Recital 79 to the DSA explains that a particular source of societal concerns contributing to the Systemic Risk Categories often stems from "advertising-driven business models" of online platforms. Amazon's advertising business is not its primary or main source of revenue nor a monetization tool for a "free" service. Instead, advertisements on Amazon help customers discover products as part of their mission to purchase consumer goods and services. Advertising helps Sellers to take new and otherwise unknown brands and products and have them be discovered by customers, as well as Sellers of known and trusted brands. Our revenues are not driven by advertising across the internet and linking customers to third-party services and websites. These elements make Amazon's advertising in the Amazon EU Store very different from advertisements on search engines or social networking services.

Advertising in the Amazon EU Store is instead an inherent part of the shopping experience in the Amazon EU Store, just as in other online or physical retail stores where retailers position products so that customers can easily find and buy them, for instance at the front of an aisle or as part of online shopping results. Amazon offers different types of placements which are clearly identifiable to customers as advertisements, using the label "Sponsored". The majority of advertising in the Amazon EU Store appears in "Sponsored Products"[29] and "Sponsored Brands"[30] placements. These typically respond to the context in search queries entered by customers or the product detail pages the customer is viewing. Customers that click on these advertisements will then be linked to product details pages or brand storefronts for the advertised products sold in the Amazon EU Store. These placements help Sellers draw customer attention to offers that best fit what the customer is looking for.

Across all Ads programs, Amazon Ads invests heavily in people and resources to protect customers, brands, advertisers, and the Amazon EU Store from fraud and other forms of abuse, including non-compliance with laws or our terms and conditions. Amazon Ads has advertising policies for the ads it publishes in the Amazon EU Store[31] which address specific regulatory requirements for each Storefront and help to maintain customer and advertiser trust. For example, products that may infringe, encourage or enable the infringement of IP or personal rights are prohibited as well as violent or offensive content. Advertisers agree to comply with Amazon advertising policies when registering to advertise in the Amazon EU Store.

To support these advertising policies, Amazon deploys a number of additional measures including: (i) automated moderation mechanisms that apply on all visible elements of an ad (including advertiser-supplied images, product listing titles and images, and product descriptions), (ii) human review, and (iii) blocking specific types of products where we have determined no advertising should be allowed. To complement these measures, we also regularly audit live ads to identify any potentially non-compliant ads and apply the learnings to this as feedback to continually improve our automated moderation tools as well as our training and processes for human reviewers. Amazon also proactively detects and takes action against advertisers that breach our advertising policies. We have dedicated teams that investigate bad actors and enforce policy violations by advertisers.

In addition to the above types of advertising, Amazon also operates programs related to marketing the Amazon EU Store. With millions of products and programs available on the Amazon EU Store, the Amazon Associates Program ("**AAP**") and the Amazon Influencer Program ("**AIP**") are two means by which Amazon drives discoverability, by making it simpler for qualifying creators (i.e., content creators, publishers and bloggers)

[29] Sponsored Products, https://advertising.amazon.com/en-gb/solutions/products/sponsored-products?ref_=a20m_us_hnav_smb_p_sp_t1

[30] Sponsored Brands, https://advertising.amazon.com/en-gb/solutions/products/sponsored-brands?ref_=a20m_us_hnav_smb_p_sb_t1

[31] Amazon Ads Guidelines and Acceptance Policies, https://advertising.amazon.com/en-gb/resources/ad-policy/creative-acceptance

("**Creators**") and qualifying influencers ("**Influencers**") to direct their audience to their recommendations on the Amazon EU Store.

- AAP helps customers discover products they may like and can buy on Amazon by enabling Creators to use easy link-building tools to direct their audience to their recommendations, and earn from qualifying purchases and programs. Creators participating in the AAP agree to the Amazon Associates Program Operating Agreement. Per the agreement, Creators must be lawfully able to enter into contracts (e.g., must not be minors). To receive the commission, a visitor to the Creator's site must make a "qualifying purchase". Qualifying purchases occur when the visitor clicks on a link on the Creator's site and subsequently places an order with Amazon. Creators can only promote products that are already available for purchase on the Amazon EU Store. As a result, AAP poses no new risk beyond those identified in this report. Historically, Creators would be able to upload content (such as profile pages and articles) onto the Amazon EU Store if they were part of the Onsite Associates Program ("OAP").

- Within the AAP, is the AIP which is specifically for Influencers. The AIP was introduced in response to the difficulties Influencers were experiencing in linking to Amazon from social media sites, which typically do not allow links out. Through the AIP, an Influencer can create a storefront with a vanity URL (i.e., a unique web address for each Influencer) that the Influencer can verbally reference or include in their profile, for their audience to find them on Amazon. This helps customers to discover products promoted by the Influencers they follow on social media. However, Influencers can only curate products that are already available for purchase on the Amazon EU Store. As a result, AIP poses no new risks beyond those identified in this Report. [Confidential]. At present, Influencer content is discoverable through the Influencer's already-engaged followers (i.e., customers who transit to an Influencer's Amazon storefront from the Influencer's off-Amazon link, or follow them on-Amazon), product detail pages, and in manual test placements.

- Unlike the AAP, the AIP permits Influencers to have their own storefront and shoppable content on Amazon with a URL to showcase the products they recommend to their followers. In the EU, the AIP currently operates in Belgium, France, Germany, Italy, the Netherlands, Poland, Spain and Sweden. Irrespective of the type of content, the AAP and the AIP only enable Creators Influencers to promote/curate products that are already on the Amazon EU Store. Therefore, these do not pose any new risks beyond those identified in this report.

- There is some risk that content posted by an Influencer could be illegal in and of itself. The Amazon EU Store moderates such content pursuant to Amazon's Community Guidelines, as well as the specific Associate Program Participation Requirements designed for these programs.[32] In addition, Influencer video content must comply with

[32] Available at https://affiliate-program.amazon.co.uk/help/operating/policies/ref=amb_link_D1ScBLj8TdSLDtXhpf63BQ_2?pf_rd_p=63225559-

(Cont'd on next page)

the Amazon Live Shoppable Videos Content Guidelines.[33] Under all these instruments, Amazon will reject content that: (a) offends, bullies, harasses or encourage behaviors interpreted as such, (b) has a sexual nature, or intends to promote sexual services, (c) harms children, by sexualizing or exploiting them, (d) promotes violence of any sort, against people or animals, (e) impersonates brands or people, of (f) violates third party's IP rights. Amazon also has a specific Amazon Affiliates Anti-Counterfeit Policy that prohibits Creators (and qualifying Influencers) from using wording such as "dupe," "fake," or "faux" in connection with a brand or knowingly promoting counterfeit products or products that infringe the IP rights of others. Amazon suspends or terminates accounts that fail to abide by this policy, including funds being withheld, and other legal consequences may also be triggered.

These existing protections and measures (in addition to those implemented for Seller listings described in Sections 3.2 and 3.3) ensure that the advertisements displayed in the Amazon EU Store meet a high standard and quality and contribute to mitigate the Illegal Content Risk.

3.5.2 **Recommender systems in the Amazon EU Store**. Amazon offers hundreds of millions of products across dozens of categories to its European customers, ranging from high-end electronics, to everyday essentials, to fashion apparel. Like all retailers – whether online or in physical stores – we need to organize the Amazon EU Store to help customers navigate what would otherwise be an overwhelming selection of products. We use recommender systems as one way of accomplishing that goal. We seek to ensure that customers can easily understand why they are seeing the product recommendations that we show to them, whether they are on an Amazon EU Store's homepage, searching for a specific product, or studying the particulars of an item on the product detail page.

Our recommender systems organize product offerings and product information in the Amazon EU Store in a way designed to help customers shop for their next pair of socks or laptop computer. They do not prioritize news articles, public health information, political opinion pieces, or spread the type of "coordinated disinformation campaigns".[34] Similarly, the goal of these recommender systems is to help customers find relevant products and complete a purchase, not to "stimulate behavioral addictions"[35] harmful to well-being.

Amazon's shopping and discovery experience features the items that it considers customers will want to view, based on real-time information about the specific customer, their past engagement (*e.g.* clicks, add-to-carts, purchases), their specific search query, or product attributes (availability, handling time, etc.), amongst other factors. The success of Amazon's shopping and discovery function is measured by surfacing products that customers intend and expect to find, and it is therefore critical to Amazon that customers

c279-45a0-9bbb-735fce57846d&ac-ms-src=ac-nav%23Associates+Program+Participation+Requirements#Associates%20Program%20Participation%20Requirements.

[33] Available at https://www.amazon.com/b?ie=UTF8&node=88213481011.

[34] Recital 83 to the DSA

[35] Recital 83 to the DSA

shopping in the Amazon EU Store find high quality and safe products that match their intent.

One of the features used by customers to find products in our Amazon EU Store is the search functionality, which is accessible at the top of nearly every page on our website and in our mobile app. Based on the entered search terms, we show customers a set of "featured" results that we think best match what the customer is looking for. Featured results consider aggregate customer actions (*e.g.*, how often an item was purchased), how well the information provided about the product (*e.g.*, title and description) matches the search query, and other factors like product availability and shipping costs when displaying search results.

The search functionality has built-in tools that can take corrective actions on a variety of search experiences that risk customer trust. For instance, if customers submit queries showing intent for infringing products (*e.g.* Searching for "[Confidential]" or "[Confidential]" on Amazon.de) Amazon blocks the visibility of auto-complete suggestions in the search bar where customers type their search queries and returns a search results page with no results. These tools are also used to remove ads and merchandising from search results pages (*e.g.*, when a customer uses the specific query "[Confidential]" or "[Confidential]"). Similarly, for certain cases where there is a potential safety or customer trust risk on certain products being recommended to a customer while shopping on the Amazon EU Store, Amazon will block the recommendation. For example, if a customer is viewing a product offer for a product containing an explosive precursor, other products containing explosive precursors will not be recommended by Amazon's systems.

The measures applicable to recommender systems in the Amazon EU Store (in addition to those implemented for Seller listings described in Sections 3.2 and 3.3) contribute to mitigate the Illegal Content Risk.

3.6 Measures to prevent reappearance of illegal content

Amazon reduces the likelihood that content once identified as illegal does not reappear on the EU Store through the continuous feedback loop of its controls. Because products in the Amazon catalogue are offered against a single listing, when an ASIN is removed either (i) proactively, (ii) following an order from a competent authority or (iii) following a notice, no Seller can list an offer for that ASIN without first successfully appealing and remediating the reason for removal. Therefore, the ASIN is not visible in the EU Store's catalogue authorization tools also function to reduce the likelihood that infringing content could reappear in the EU Store because they limit authorizations for the creation of new product branded listings to the brand owner, Amazon, and qualified Sellers. This means that a Seller without authorization cannot create a new listing for a branded item. [Confidential]

However, bad actors may seek to circumvent an ASIN removal by, for example, re-listing the same product under a different brand or product identifier. Therefore, our strategy for protecting the Amazon EU Store includes establishing durable and continuously operating proactive controls that remove content identified as illegal. These controls, including text, image, and product listing rules, also prevent the reappearance of content that has previously been removed and which the

rule was designed to target. The investments in these proactive controls are undertaken on Amazon's voluntary own-initiative, as the DSA reaffirms that intermediaries have no general monitoring or active fact-finding obligations.

Amazon constantly monitors and evaluates new ways bad actors could use to circumvent Amazon's measures, including the incidence of violations by Sellers who repeatedly upload infringing or non-compliant content. Amazon operationalizes this strategy by ensuring that Amazon moves controls from a post-listing to a pre-listing stage, launching proactive Product Listing Rules for products that were in scope of recalls (e.g. children's digital cameras). Amazon has taken significant action to prevent the re-listing of recalled products, including by removing unsafe ASINs, identifying the root causes of recalled ASINs persisting in the Amazon EU Store (e.g., human error, brand name misspelling, or evasive listing), planning actions to prevent the risk of similar products being listed (e.g., by re-training associates on complex cases, reviewing the attribute combination used for ASIN review and classification, and expanding the keyword search criteria in implementation of product listing rules), and coordinating potential follow-up Seller enforcement actions.

As mentioned above, RISC is responsible for identifying Sellers that repeatedly violate the same policy multiple times over a period of time.

Similarly, Brand Protection tracks the number of repeat suspended Sellers, i.e., Sellers that have been suspended for policy violations and reinstated following a Seller appeal, and which are subsequently suspended again as a result of IP infringement or abuse. Learnings from tracking these repeat suspended Sellers help us identify abusive behavioral patterns and inform improvements in upstream Seller account suspensions.

3.7 A-to-z guarantee and return policy

In addition to the measures and protections in place to protect customers from inauthentic and unsafe products, Amazon aims to provide a single return policy for customers to enable them to purchase with confidence regardless of whether they purchase from Amazon Retail or a third-party Seller. Amazon provides the A-to-Z Guarantee to customers who purchase products from third-party Sellers, so they can get a full refund for any item that does not arrive in the condition expected or on time. For purchases made from Amazon Retail, customers have equivalent return and refund rights under the Amazon EU Store return policy. In 2024, Amazon expanded the A-to-z Guarantee to include customer claims for property damage and personal injury caused by defective physical products. For property damage and personal injury claims, the A-to-Z Guarantee applies to all physical products sold in the Amazon EU Store, regardless of whether they were purchased from Amazon Retail or a third-party Seller. In addition to the A-to-z Guarantee and the Amazon EU Store return policy, if we identify that a customer purchased a counterfeit or recalled product, Amazon proactively contacts the customer, informs them that they purchased a counterfeit product, and fully refunds their purchase – without the need for the customer to take any action. The A-to-z Guarantee and the Amazon EU Store return policy contribute to mitigating the severity of the Illegal Content Risk, providing a remedy in the rare event a customer purchases an inauthentic or unsafe product.

4. Assessment of Fundamental Rights Risk

Article 34 of the DSA requires assessment of actual or foreseeable negative effects for the exercise of certain fundamental rights, in particular human dignity (Article 1 of the Charter of Fundamental Rights of the European Union (the "**Charter**")), respect for private and family life (Article 7 of the Charter), protection of personal data (Article 8 of the Charter), freedom of expression and information, including the freedom and pluralism of the media (Article 11 of the Charter), non-discrimination (Article 21 of the Charter), respect for the rights of the child (Article 24 of the Charter) and a high level of consumer protection (Article 38 of the Charter).

To recall, Amazon's assessment of "actual or foreseeable negative effects on the exercise of fundamental rights"[36] has been has been conducted on the basis that the DSA does not introduce a novel concept of fundamental rights over and above those rights which are recognized as binding in the Union legal order, which are primarily those fundamental rights of individuals or legal persons protected by the Charter, in accordance with the case law of the Court of Justice of the European Union and the European Convention on Human Rights. While fundamental rights are enforceable only *vis-à-vis* the EU Institutions and Member States, Amazon has considered foreseeable negative effects relevant to the principles underlying these rights.

For the purposes of this Risk Assessment, we have focused on analyzing any actual or foreseeable effects on the right to consumer protection which might be affected by the design, functioning and use of the Amazon EU Store. For completeness, we also assessed other relevant rights referred to in the Charter, such as freedom of expression, rights to property, human dignity, non-discrimination, and data protection.

As a retailer operating a store selling consumer goods, the risks and potential negative effects to fundamental rights relevant to the Amazon EU Store are different from other business models subject to Chapter III, Section 5, of the DSA. To the extent any such risks exist on the Amazon EU Store, they are no different to or greater than risks present on any online retail business. In particular, the information available in the Amazon EU Store is commercial in nature and relates exclusively to the products available in the Amazon EU Store for sale to adults, limiting any potential impact on the fundamental rights enshrined in the Charter and identified in Article 34. Amazon has analyzed actual or foreseeable negative effects for the exercise of fundamental rights in this context and has identified no actual or foreseeable negative effects for the exercise of certain of these enumerated rights. For example, Amazon is not a platform for exchange of content about private and family life, nor is it foreseeable that a service facilitating the sale of products would be used or misused in a manner negatively influencing the right to private and family life. Neither has Amazon observed actual negative effects on the right to private and family life stemming from the use or misuse of the Amazon EU Store.

Amazon has always strived to protect its customers and Sellers from any measures or behavior which would actually or foreseeably negatively affect the enjoyment of those rights whether or not they can be said to be directly enforceable against Amazon as a matter of the strict application of the Charter. This approach goes hand in hand with Amazon's overall mission of creating a trustworthy and safe online retail environment which respects the fundamental rights of its customers and Sellers. On this basis, Amazon's risk assessment has carefully identified and analyzed possible permutations or manifestations of relevant risks that can be considered, as a

[36] DSA, Article 34(1)(b).

general matter, to have actual or foreseeable negative impacts associated with the enjoyment of fundamental rights as defined by the DSA.

Below we set out an assessment of potential negative effects for the exercise of certain fundamental rights in the context of the Amazon EU Store and discuss how Amazon manages competing impacts to fundamental rights when assessing risks and appropriate mitigation measures.

4.1 Consumer protection

Amazon strives to be the world's most customer-centric company. As described in this Risk Assessment, our investments and industry leading controls protect customers from unsafe and infringing products, fraud, abuse, and offensive content.

Amazon's experience in risk assessment and mitigation measures suggests that consumer harm can result from illegal goods sold on its Amazon EU Store. Amazon does not have evidence that risks to consumer protection exist that are different from the risks related to the Illegal Content Risk category (as, for example, would be the case for social media and content sharing platforms whose business model is not transaction-based). Indeed, by virtue of its transaction-based business model, Amazon's risks cannot be disassociated from the goods sold on its Amazon EU Store. Therefore, Amazon's risk assessment with regard to consumer protection is integrated into its assessment concerning the Illegal Content Risk (see section 3).

Ensuring consumers are adequately protected when they shop in the Amazon EU Store is critical to Amazon's success. As is set out in detail above, Amazon has invested enormous time and resources into developing sophisticated tools for monitoring and assessing its compliance with various regulatory frameworks for consumer protection, including by protecting its users against bad actors, by protecting them from counterfeits (Brand Protection), protecting them from illegal or unsafe products (Product Safety and Compliance); and protecting them against fake or incentivized reviews (Trustworthy Reviews).

Due to our robust measures and protections, only rare occurrences remain when a customer's experience is negatively impacted by fraud or abuse. And in these cases, customers are protected by our A-to-Z guarantee and return policy. The Amazon EU Store is designed and functions to deliver a high level of consumer protection.

4.2 Offensive and controversial products

Amazon's goal is to provide a great shopping experience by offering its customers the biggest selection of authentic and safe products on Earth at competitive prices with convenient delivery. Amazon strives to provide customers a space where they can find and discover anything they might want to buy online, even if Amazon does not agree with the message conveyed by some of the products or the personal views of the Seller. We strongly support freedom of expression, while protecting customers against potential abuse and negative effects to their human dignity and right to non-discrimination. This is the basis for our offensive and controversial product policies. In 2024 until July, Amazon removed over 3.1 million products for violating the controversial product guidelines. The vast majority of these products were identified, reviewed, and removed proactively by our automated tools, often before they are seen by a customer. We ensure controls supporting

consumer protection and potentially impacting freedom of expression and other fundamental rights are implemented fairly and proportionately consistent with our strategic aims.

4.2.1 **Proactive controls**. Amazon prohibits the sale of products[37] and books[38] that (i) promote, incite, or glorify hatred, violence, racial, sexual, or religious discrimination or promote organizations with such views; (ii) contain pornography, glorify rape or pedophilia or promote the abuse or sexual exploitation of children; or (iii) graphically portray violence or victims of violence, and advocates terrorism; among other material deemed inappropriate or offensive. Just like any other retailer or bookseller who decides what to offer in its store, Amazon carefully considers the types of content that can be made available in the Amazon EU Store.

To enforce our offensive and controversial product policies, in 2024, we:

- Leveraged machine learning and automation to filter listing submissions that we suspected of potential policy violation, and then manually "walked the store" to review these. In 2024, we manually reviewed an average of 15,000 listing changes each day to ensure compliance with our policies.
- Removed over 2.6 million products for violating our controversial product guidelines, the vast majority of these products are identified, reviewed, and removed proactively by our automated tools, often before they are seen by a customer. The realm of potentially offensive products and books is nuanced and diverse, and Amazon reviews thousands of products every day against Amazon policies. Amazon periodically reviews and updates these policies to ensure there is a proportionate balance between offering a wide product selection to customers and protecting the freedom of expression of manufacturers and copyright owners, based on experience, current events, and other relevant developments, and in consultation with internal and external resources.

4.2.2 **Mechanisms to moderate offensive and controversial products**. Amazon has a dedicated team responsible for developing and updating our policies and refining and maintaining the proactive controls that continuously monitor the Amazon EU Store. This team considers input from customers and consults resources issued by civil rights and anti-hate organizations to inform updates to applicable guidelines. For example, Amazon created a policy to prohibit products with [Confidential].

As a company, we embrace the fundamental human rights of freedom of expression and information. As a bookseller, we have chosen to offer a very broad range of viewpoints, including books that may conflict with our values and corporate positions. [Confidential]. Customers and other members of the public can report content that may violate our guidelines by using the "Report an Issue" feature at the bottom of a book's detail page on Amazon, and they also can reach out to Customer Service. We promptly investigate any book when a concern is raised.

[37] Offensive and Controversial Materials, https://sellercentral.amazon.de/help/hub/reference/external/GQKVFBUXQJ4FR2G9?locale=en-US

[38] Content Guidelines for Books, https://www.amazon.nl/gp/help/customer/display.html/?nodeId=GJUAA7A28KBJE2YV&language=en_GB

4.2.3 **Holding bad actors accountable**. If we determine a product violates our policies, we remove it immediately and may take action on the Seller account involved, including suspending or banning an account or withholding payments.

4.2.4 **Preventing amplification**. We prohibit certain content from appearing on the Amazon EU Store landing page in order to prevent content that could be controversial or offensive to some customers from being amplified. This includes adult products (such as sexual wellness, family planning products), tobacco/hemp-related products, toy guns, and scatological themed products. Similarly, our global advertising policy, which applies to all advertising placements on the Amazon EU Store, prohibits certain content from all ads to comply with laws and prevent potentially controversial or offensive content from being amplified to customers. This includes, for example vulgar or obscene language or language containing profanity (including obscured profanity, graphic or suggestive language or double entendres) and content that encourages, glamorizes or depicts excessive consumption of drugs or alcohol.[39] Using automation, Amazon prevents Sellers from purchasing ads including prohibited, offensive, vulgar, and hateful language. To ensure that certain sensitive categories of products are not surfaced by ads, Amazon also prohibits advertising products in a number of categories, including weapons permitted to be sold in the Amazon EU Store, tobacco and tobacco-related products.

4.3 Fair and objective moderation of content in the Amazon EU Store

Generally, all content published on the EU Store (including text, photos, videos, or links) must comply with Amazon's Community Guidelines.[40]

Amazon aims to efficiently, objectively, and fairly moderate content in the Amazon EU Store. Thus, Amazon's focus is to strike the right balance between the severity of the policy violation and corresponding enforcement action, minimize mistakes (in both over and under enforcement), and monitor accuracy to avoid negatively affecting legitimate Sellers' and customers' freedom of expression.

Further, Amazon is bound by the Platform-to-business regulation ("**P2B Regulation**"), which similarly aims to create a fair, transparent, and predictable business environment for traders on online platforms.[41] As the DSA does not in principle identify any risks to the rights of traders that are not already addressed by the P2B Regulation, there is no reason to think that the protection afforded under the P2B Regulation would not be sufficient for traders using Amazon's service.

4.3.1 **Proportionate proactive controls**. Prior to implementing new proactive controls (*e.g.* a machine learning model that identifies use of a trademarked term on the product listing page and removes it as potentially infringing content), Amazon's content moderation teams test the precision of the control. Amazon does not implement controls that would

[39] Prohibited Content, https://advertising.amazon.com/en-gb/resources/ad-policy/creative-acceptance/prohibited-content?ref_=a20m_us_spcs_cap6_spcs_cap5

[40] Available at https://www.amazon.nl/-/en/gp/help/customer/display.html?nodeId=GLHXEX85MENUE4XF.

[41] As described in Recital 52 to the P2B Regulation, the P2B Regulation "seeks to ensure full respect for the right to an effective remedy and to a fair trial as laid down in Article 47 of the Charter of Fundamental Rights of the European Union and promote the application of the freedom to conduct a business as laid down in Article 16 of the Charter."

disproportionately and inaccurately impact non-infringing listings or safe and compliant products.

4.3.2 **Transparent content moderation tools**. In February 2023, Amazon launched Account Health Rating ("**AHR**"),[42] a new feature to enhance transparency. AHR responds to a few key pieces of feedback from Sellers. First, rather than a list of policy violations that could lead to suspension of their account, Sellers have asked to understand exactly where they stand overall and which policy was violated. The new AHR is a data-driven and holistic metric that contains a numerical score (0 to 1000) and computes factors for account suspension based on accumulated policy violations.[43]

Second, if there are any outstanding policy violations negatively impacting the AHR, a Seller will be able to see the level of severity for each violation, ensuring that they can prioritize the most important issues first.

Third, Sellers have asked for more help in adhering to our policies, so when a Seller's account is at-risk, dedicated account health specialists will proactively call, email, and send notifications to the Seller to discuss and support the Seller in getting their account back on track.

4.3.3 **Fair enforcement and redress**. Recital 81 to the DSA identifies the potential for "submission of abusive notices or other methods for silencing speech or hampering competition" to negatively affect expression. Amazon seeks to mitigate the potential for this kind of abuse to negatively impact Sellers. For example, some rights owners pursue overenforcement of their protected IP rights against fair use or submit abusive notices to harm competitors. Amazon's expert investigators are armed with IP information provided through Brand Registry and robust training to objectively evaluate infringement claims, and do not enforce against non-infringing content.

When we remove a listing or suspend a Seller's account due to a policy violation, we provide clear and actionable communications describing the policy violation that led to the enforcement action. Sellers can remediate the policy violation and appeal the enforcement, or dispute the enforcement and ask Amazon to re-examine the decision. If Sellers remain dissatisfied with an Amazon decision after reaching out to our support teams, they can seek resolution for most disputes through an independent mediation process, facilitated by the Centre for Effective Dispute Resolution. These redress mechanisms enhance Amazon's ability to appropriately protect Sellers' interests and expression. We also have organized teams dedicated to ensuring that we hear and address Seller pain points. For example, the

[42] Account Health Rating Program Policy, https://sellercentral.amazon.de/help/hub/reference/external/G200205250?locale=en-US

[43] AHR includes Amazon Anti-Counterfeiting policy, https://sellercentral.amazon.de/gp/help/external/G201165970?locale=en-US; Amazon Brand Name policy, https://sellercentral.amazon.de/gp/help/external/2N3GKE5SGSHWYRZ?locale=en-US; Amazon Intellectual Property policy, https://sellercentral.amazon.de/gp/help/external/G201361070?locale=en-US; Customer Product Reviews Policies, https://sellercentral.amazon.de/help/hub/reference/external/GYRKB5RU3FS5TURN?locale=en-US; and Category, product, and content Restrictions, https://sellercentral.amazon.de/gp/help/external/G201743940?locale=en-US.

Small & Medium Business Empowerment team is constantly seeking feedback from small and medium businesses to improve the Seller experience.[44]

4.3.4 **Educating Sellers**. To help Sellers offer only permitted content and products and deliver on a great customer experience, Amazon helps adhere to our policies through education. Seller content in the Amazon EU Store is provided in at least ten languages, including in the languages of each Storefront as well as in Chinese and Korean. Amazon's Seller News team also notifies Sellers of policy, tool, and program updates and changes regularly to help Sellers stay ahead of these changes and improve overall selling experience.

4.4 Maintaining customer trust through privacy

As described above, it is fundamental for Amazon to provide a safe and trustworthy user experience for Amazon EU Store users, including by maintaining the privacy of users' personal information. We are highly focused on our obligations under the EU's General Data Protection Regulation **("GDPR"),** which sets out the primary EU law requirements for data protection, and we have a long history of implementing robust compliance procedures to safeguard the right to data protection of our customers and deliver compliant solutions to the Amazon EU Store users. We have continued this work over the past 12 months, since the completion of our 2024 Risk Assessment.

When assessing data protection risk—similar to the assessment of other risks in this report— it is important to recall that the Amazon EU Store is an online retail service. Amazon customers use the Amazon EU Store to search for, purchase, and obtain products from third-party sellers quickly and easily. The design and functioning of the Amazon EU Store is therefore focused on facilitating commercial transactions in these products, including storing them in physical warehouses and getting them to customers through a physical logistics operation. This distinguishes the Amazon EU Store from the purely digital business models pursued by most other VLOPs. Customers do not use the Store to store and disseminate content to the public in ways that would raise risks around the amplification of disinformation or other illegal content, or intentional manipulation of the service. Likewise, the Amazon EU Store business model does not seek to encourage users to engage with content in order to serve them ads and therefore does not contribute to the viral dissemination of content.

In light of our role as an online retailer, our Risk Assessment – and thus the content of this report –focuses on those Systemic Risk Categories that pose the greatest potential probability and severity of harm to Amazon EU Store customers, such as the risks of illegal content, unsafe products, and false or deceptive customer reviews. In addition, however, we also have carefully considered the data protection risks relevant to the Amazon EU Store, as required by Article 34(1) DSA. Where data protection-related risks do arise, we describe these – and our mitigations – below.

4.4.1 Risk assessment and mitigation steps

The operation of the Amazon EU Store involves the collection and processing of personal data, including data that we use in order to show customers products that might be of interest to them.

[44] Amazon European Small and Medium Enterprises Impact Report, https://assets.aboutamazon.com/51/f6/01cca00a4447830799f028a0f0b4/amazon-sme-report-2022-eu.pdf

We also hold personal data about Amazon EU Store customers that our customers are likely to perceive as being more sensitive in nature, including financial data, as well as data about their purchases on the Amazon EU Store. Our customers reasonably expect us to store their data securely and to use it responsibly. For this reason, our Risk Assessment focuses on those data protection risks that have the highest combination of probability of occurring and potential severity of harm, in light of the actual data collection and processing that we do of customer data. In conducting the risk assessment required by Article 34 DSA, we have identified and focused in particular on the following potential risks to data protection:

(i) **Security (risks of personal data theft or misuse)**

I Risks

We collect a range of data about Amazon EU Store customers in order to provide our services and ensure their experience on our Amazon EU Store is optimal. Some of this data, such as customers' financial details, is potentially sensitive, and could be attractive to malicious actors. In conducting this risk assessment, we have recognized that customers could therefore be harmed if we failed to store their personal data securely or otherwise mishandled it, or if we failed to take adequate steps to prevent unauthorized access to or use of such data.

II Mitigations

To address the risks described above, we design all our products, services, and systems with privacy and security in mind. We employ thousands of professionals whose sole mission is to ensure the integrity and security of customer data, including a world-class team of security experts monitoring our infrastructure 24/7 to protect our customers. For example, we deploy data handling and data classification standards that require Amazon employees and contingent workers to apply appropriate security controls to customer data and to handle that data appropriately throughout its lifecycle (i.e., from its creation to its destruction or deletion).

We maintain physical, electronic, and procedural safeguards in connection with the collection, sharing, and storage of customer data. We also use proven encryption protocols and software to protect the security of personal data during transmission, and we take appropriate steps to validate the third parties to whom customers request to port their data to further ensure our customers' security. Each of these measures is reinforced by internal-facing policies, [Confidential].

The Amazon EU Store also benefits from the underlying privacy and security capabilities of Amazon Web Services ("**AWS**").[45] AWS' core infrastructure is designed to satisfy the security requirements for military, global banks, and other high-sensitivity organizations, and it includes sophisticated technical and physical measures to prevent unauthorized access.

In addition to our own internal security processes and procedures, we work to educate customers on how they can help keep their account information private with simple steps, such as creating

[45] AWS is certified to the highest security standards for protecting the privacy of customers' data, including (but not limited to): ISO/IEC 27701 Certificate, ISO/IEC 27018 Certificate and SOC 2 Report. AWS also adheres to the CISPE Data Protection Code of Conduct.

strong, unique passwords and using multi-factor authentication or passkeys. Alongside these practical steps, our Authentication Standard sets out the authentication requirements for customer-facing applications and services.

(ii) **Transparency (lack of customer understanding of our data collection and processing)**

I Risks

Much of the personal data that we process in connection with the Amazon EU Store is data that our customers actively provide when they open an Amazon account. This includes their name, shipping address, payment details, and related information that we need in order to process their purchase orders. In addition, in order to help customers find products they might be interested in, among the millions available on the Amazon EU Store, Amazon also collects and processes other types of personal data, such as our customers' search, browsing and purchase history, among other data points. Although shoppers today generally expect online retailers to recommend products to them based on such information, we also recognize that it is important that we are transparent about this data collection, and about how we use customer data, so that customers understand our practices. Lack of transparency gives rise to the risk that customers will have questions about what data we are collecting and for what purposes.

II Mitigations

We strive to make it easy and intuitive for customers of the Amazon EU Store to learn more about how Amazon collects, uses, and shares their data. We do this by setting out information about our data processing practices in several disclosures, including but not limited to: (i) the Amazon Privacy Notice[46] (accessible at the bottom of nearly every page on the Amazon EU Store, the Privacy Notice gives customers meaningful information on the personal data that Amazon collects, the purposes for which Amazon processes that data, the third parties with whom Amazon might share the data, for how long Amazon retains customer data, and Amazon's use of personal data for advertising); (ii) the Interest-Based Ads notice[47] (accessible at the bottom of nearly every page on the Amazon EU Store, provides customers with information on how we use their data to personalize ads as well as other information, such as the data points Amazon uses to decide which ads to show them and the controls customers have over such use); (iii) the Cookie Notice and Cookie Preferences page[48] (which explains to Amazon EU Store customers the different types of cookies that Amazon uses, the purposes that these cookies serve, how long they remain on a user's device, and the steps users can take to delete them or limit their use); and (iv) Finding Products in the Amazon EU Store page[49] (which explain to Amazon EU Store customers how Amazon shows them products that Amazon thinks they might be interested in, based on factors such as their past purchases; customers can opt out of seeing product recommendations via the 'Your Account' page). We are also focused on being responsive to evolving regulatory guidance setting out best

[46] https://www.amazon.de/-/en/gp/help/customer/display.html?nodeId=201909010&ref_=footer_privacy

[47] https://www.amazon.de/-/en/gp/help/customer/display.html/?nodeId=G64JFZVFDY66XG9K

[48] https://www.amazon.de/-/en/privacyprefs/retail

[49] https://www.amazon.de/-/en/hz/cs/help?nodeId=GSUNWNFT2ALMPR3L

practices on transparency and we regularly review and update, as appropriate, the notices that we provide to customers about our data processing practices and their rights. For example, we recently updated our EU-facing Privacy Notice and also introduced changes to the information we provide when responding to data subject access requests from our customers.

(iii) **Customer controls (perceived loss of control)**

I Risks

Related to being transparent about our data processing practices, we also recognize that it is important to our customers that they have choices over the data we collect about them and how we use that data, in particular when we use that data to advertise or recommend products to them, or otherwise to personalize their on-site experience. We believe that providing customers these choices to is important to meet their high expectations when they shop in the Amazon store.

II Mitigations

In recognition of the importance of providing customers with choices over how we use their personal data, we allow them to remain in control by exercising their preferences on the Amazon EU Store. To that end, the Amazon EU Store gives customers choices over how their data is used and makes it easy for them to control such use. This is evident on various pages available to our customers on the Amazon EU Store, including but not limited to: (i) the Ad Preferences and Transparency page[50] (accessible to customers via a link in the Interest-Based Ads notice and the Privacy Policy. This page gives Amazon EU Store customers the option of either turning off all display of personalized ads to them, or limiting the types of data that Amazon uses to show them such ads); (ii) the Cookie Preferences page[51] (which allows customers to accept or decline cookies and make more granular choices about both Amazon advertising cookies and third-party advertising cookies); and (iii) the Recommendation Preferences page[52] (which allows customers to opt out of seeing recommendations when shopping on Amazon) and (iv) Data used between services page[53] (which allows customers to choose how we use their personal information across Amazon services).

(iv) **Data governance**

To ensure that we abide by our data protection commitments, and that we maintain customer trust, Amazon has adopted a number of robust data governance processes and practices. [Confidential]. We also require relevant Amazon personnel to undergo regular privacy-related training to ensure that privacy knowledge and awareness is maintained throughout our organization.

4.5 Helping Sellers to conduct their business

[50] https://www.amazon.de/adprefs

[51] https://www.amazon.de/-/en/privacyprefs/retail?oCT=ads

[52] https://www.amazon.de/-/en/privacyprefs/retail/recommendations?ref_=ya_pc_d

[53] https://www.amazon.de/-/en/privacyprefs/datause?ref_=ya_pc_datause

Although Sellers do not have a fundamental right to conduct a business using Amazon[54], we are committed to helping Sellers conduct their business smoothly on the Amazon EU Stores in line with our overall approach to create and maintain a healthy and effective partnership with our Sellers. Amazon not only protects Sellers from abuse, but also makes it as easy and straightforward as possible for legitimate Sellers to open an account and start their activity on the Amazon EU Store. We continuously strive with our tools and mechanisms, described above, to maintain a balance between deterring unwanted or unlawful behavior, on the one hand, and safeguarding Sellers' ability to successfully conduct their business on the Amazon EU Store, on the other. In this regard, in identifying and analyzing fundamental rights impacts, it is moreover important to bear in mind that the safeguarding of such rights must be commensurate to the obligations the same rights holders have towards others. Therefore, Sellers' contractual rights in their relationship with Amazon go hand in hand with their obligations towards our customers, which Amazon also has a responsibility to safeguard with proportionate and effective measures.

While there are some limitations on a Seller's ability to sell its products on the Amazon EU Store, as described comprehensively in Section 3.1 above, these are necessary to protect customers and Sellers from abusive behavior. Also, Amazon communicates with potentially non-compliant Sellers and examines potential problems by engaging in constructive dialogue with them, evaluates the accuracy and proportionality of moderation activities and enforcement decisions against potentially non-compliant Sellers.

Moreover, teams within Amazon responsible for enforcing policies applicable to Sellers seek to ensure the policies are applied diligently and accurately. As one core measurement of accuracy, these teams regularly conduct false positive and false negative audits and seek to understand the root cause of inaccurate identification of prohibited listings and listing content. The learnings from these false positive and false negative audits are then applied to improve enforcement accuracy and coverage. In this way, these audits help reduce the risk that Sellers face inaccurate removal of listings or other content.

Amazon also regularly reviews key performance metrics used to assess the risk that Seller content is inaccurately removed or Seller accounts are inaccurately suspended due to identification by IPP, or inaccurate enforcement of other policy violations through false positive audits. While Amazon aims to be highly accurate and proportionate when enforcing Seller content and accounts, we do not always get it right. We measure false positives based on statistically significant audits of enforcement decisions that consider new evidence and contacts with Sellers (e.g., an ASIN is removed and that removal is found to be inaccurate upon investigation following a Seller appeal), among other data points. Overall, however, the false positive rates show that Amazon's enforcement accuracy is very high. These metrics include:

- [Confidential].

[54] Amazon's relationship with Sellers are private-law relationships which are entered into on the basis of freedom of contract and are governed by agreed contractual terms. The Charter cannot be interpreted as providing for or creating such a standalone fundamental right that is enforceable against private business partners. And the DSA does not create such a separate right to conduct a business applicable between VLOPs and traders.

- [Confidential].
- [Confidential].

5. Assessment of Democratic Process Risk

Article 34 of the DSA requires assessment of actual or foreseeable negative effects on the Democratic Process Risk. In this regard, the Democratic Process Risk relates almost exclusively to attention-based services designed for the dissemination of information and content such as social media and, to a lesser extent, search services. The recitals to the DSA do not mention transactional business models such as Amazon EU Store as a source of such concerns. Similarly, the Commission's communication 'Shaping Europe's Digital Future' from February 2020 raised concerns about the Democratic Process Risk stemming from public debate and political campaigning and advertising moving online. Risks associated with marketplaces or retailers were not identified in this context.

As discussed in Section 3.5 above, in view of Recital 79 to the DSA, Amazon finds that an important distinction critical to assessing relevant risks in this context is whether the business model consists of the dissemination of content and information financed mainly by displaying advertisements, or whether it consists of a transactional platform for the sale of goods financed through commission fees paid by Sellers.

The Amazon EU Store does not distribute content such as general speech or personal videos produced or shared by users and is not a venue for exchange of civic discourse, democratic processes or other electoral activity, or for dissemination of content that could impact public security. While the Amazon EU Store offers advertising, it relates almost exclusively to products being offered for sale. In contrast to attention-based, advertising-funded social media platforms, advertising on the Amazon EU Store is only ancillary to its main activity of online retail and functions to helps customers discover, navigate, and compare offers, rather than simply being a means by which to monetize page views. Moreover, the Amazon EU Store does not host political advertising that could propagate messaging on issues such as politics or matters of concern to public security.

Therefore, by virtue of the nature of Amazon's business model, there is no foreseeable prospect of activities that could give rise to the Democratic Process Risk taking place in the Amazon EU Store. Amazon has also not identified such coordinated disinformation campaigns with potential negative effects on Democratic Process in the Amazon EU Store, as they simply do not occur on the Amazon EU Store.

6. Assessment of Public Health Risk

Article 34 of the DSA requires assessment of actual or foreseeable negative effects on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence. Recital 83 to the DSA refers to Public Health Risks stemming from activities including "coordinated disinformation campaigns related to public health". Drawing on the analysis set forth in Section 5 with respect to the Democratic Process

Risk, the risk of a disinformation campaign leading to negative effects for the Public Health Risk is more relevant for a service where the business model consists of the dissemination of discourse and information relevant to health topics.

Unlike social media platforms, Amazon is not a forum for the dissemination or amplification of content, and its business model is not attention-based, *i.e.* it does not measure its performance based on the amount of time a user spends on its site. In fact, Amazon's business model is better articulated as targeted at the 'de-amplification' of any relevant risks on its marketplace rather than stimulating behaviors that accentuate public health risks. For these reasons, it is not possible for a bad actor to use Amazon for "a disinformation campaign related to public health".

Similarly, the Amazon EU Store is unlikely to lead to serious negative consequences to a person's physical and mental well-being by, for example, deploying an online design to "stimulate behavioral addictions" of users. Just as with any store, the Amazon EU Store is designed to help customers find what they are looking for, compare offers, and make an informed purchase decision. Amazon EU Store does not profit from customers spending time on the platform, but by purchasing goods they are interested in. Amazon is therefore incentivized to provide customers with a safe, reliable, and authentic customer experience in order to build strong and lasting customer relationships.

As a result, our risk assessment has not uncovered any evidence of there being a realistic prospect of the Amazon EU Store posing a "systemic" risk because it does not distribute content that can be consumed just by navigating the Amazon EU Store, nor does it host advertising that could propagate messaging on public health issues.

To the extent that negative effects to public health, or a person's physical and mental well-being could arise through the sale of products or services sold on Amazon, we address these risks as part of our assessment of Illegal Content Risk and our measures to ensure only safe and authentic products are sold on Amazon in Section 3; as well as in Section 4, which addresses the Fundamental Rights Risk, for example through the sale of controversial products. By preventing the appearance of dangerous or counterfeit products on the Amazon EU Store, any risks to public health are simultaneously addressed.

While Amazon cares deeply about the protection of minors, the Amazon EU Store is not designed for or directed at minors, nor is Amazon aware of evidence suggesting that the Amazon EU Store is used by a measurable number of minors. The Amazon EU Store does not sell products or services for purchase by minors or target minors through marketing or advertising. Although the Amazon EU Store offers children's products (such as toys or children clothes), they are offered for purchase by adults. The Amazon EU Store is similarly unlikely to be accessed and used by minors under 18 due to the nature and content of the service, the way in which the service is accessed, and the measures Amazon has put in place. When customers set up an Amazon account they agree to terms that prohibit minors from making purchases on the Amazon EU Store without the involvement of a parent or guardian.[55] Additionally, customers must also have a valid payment

[55] Amazon EU Store's Conditions of Use and Sale, https://www.amazon.de/hz/cs/help?nodeId=GLSBYFE9MGKKQXXM. Amazon EU's Privacy Notice, https://www.amazon.de/gp/help/customer/display.html/ref=s9_acss_bw_cg_PR0518_md3_w?nodeId=201909010&

(Cont'd on next page)

method such as a credit card linked to their account in order to purchase products or services on the Amazon EU Store.[56] Amazon EU Store is in any case configured to have appropriate and proportionate measures in place to ensure that the risks to any minor accessing the Amazon EU Store are low. For example, Amazon has a procedure to take action on Amazon accounts where evidence is received that the account has been created by a child, including closing the account. Age verification is applied to the purchase and delivery of restricted items (for instance, alcohol) depending on local law. Content moderation measures govern inappropriate content prohibiting advertisement targeted at or appealing to minors, as well as inappropriate or offensive content appearing on the Amazon EU Store.

By virtue of the nature of Amazon's business model and its robust controls, activities that could give rise to the risks described by the Public Health Risk are unlikely to take place in the Amazon EU Store, and have not been identified based on Amazon internal data and observations.

7. Conclusion

The Amazon EU Store is designed to serve customers by providing the best combination of selection, price, and customer experience to help customers discover and purchase physical goods, and ensure a customer's satisfaction with their purchase. Amazon believes that if customers have good experiences, they will return to Amazon for future purchases. Conversely, when customers' expectations are not met, they are unlikely to return to Amazon and will shop at other retail stores instead. This direct economic feedback gives Amazon strong incentives to ensure the information presented in the Amazon EU Store is accurate and trustworthy and the products offered for sale comply with all applicable laws.

As described in this Risk Assessment, Amazon has deployed four strategic aims to effectively and proportionately mitigate potential negative effects on the Systemic Risk Categories stemming from the use or misuse of the Amazon EU Store service. To the extent risks arise in connection with the Amazon EU Store, Amazon considers that the mitigating measures described above are reasonable, proportionate and effective to address them, and protect the integrity of the Amazon EU Store, legitimate Sellers, and consumers.

In Section 2.1 of this Risk Assessment we introduced a number of Amazon's unique ways of working. Another one of these is our "Day 1" mentality. Day 1 is about being constantly curious, nimble, and experimental. It means being brave enough to fail if it means that by applying lessons learnt, we can better surprise and delight customers in the future. Consistent with that mentality we know that delivering for customers means continuously evaluating and adjusting our approach to effectively manage our business and that we must resist complacency. We know it is critical for us to adapt quickly to changing external risks and to the ever-evolving needs of our customers by innovating on their behalf. While we do not believe that Amazon's approach is the only one,

pf_rd_m=A3P5ROKL5A1OLE&pf_rd_s=merchandised-search-2&pf_rd_r=461Z2KJYVNQWBGK9CMKG&pf_rd_t=101&pf_rd_p=3713bd31-a173-4eda-b64e-d02c7396f114&pf_rd_i=14856936031, which is also brought to a customers' attention when they set up an Amazon account, contains the same prohibition.

[56] Having a credit or debit card linked to the account is one indicator that the account is likely owned by an adult, as financial institutions would require someone to be above legal age or acting under parental consent to enter into the agreements necessary to hold a credit or debit card.

we are proud of the progress that we have made in our risk controls and will continue to invest to protect the Amazon EU Store and customers from all forms of abuse and fraud.