Amazon – Written evidence (FDF0073)

Amazon UK retail business welcomes the opportunity to submit written evidence to the Fraud Act 2006 and Digital Fraud Committee. This response sets out background on Amazon in the UK, our approach to combatting fraud as well as answering specific questions posed by the Committee.

About Amazon

Amazon strives to be Earth's most customer-centric company, where people can find and discover the widest possible selection of authentic goods. Today, we have hundreds of million active customer accounts and over 1.9 million selling partners worldwide. In the UK, this equates to more than 65,000 small and medium sized enterprises (SMEs) who grow their businesses by selling their products in Amazon's stores across the world, achieving over £3.5 billion in exports. We are proud to help these businesses thrive and create new jobs in their local communities, leading to 175,000 indirect jobs created in the UK alone.

Whether we are innovating on behalf of millions of customers, building a convenient working environment for our employees or supporting local communities, our role as a force for good in the countries where we operate is always a top priority.

Our mission is to continually raise the bar on customer experience, pushing the boundaries of consumer choice and convenience while also helping to drive digital empowerment, technology innovation, and productivity wherever we operate. As part of this, we work hard to earn and maintain customer trust, and strictly prohibit the sale of counterfeit products, while being absolutely committed to protecting our customers from fraud and abuse. Last year we published our first Brand Protection report[1], which sets out how we ensure customers around the world shop for authentic products in our store, and how we protect brands and the millions of SMEs that sell authentic products on our marketplace.

The threat from fraud

According to the National Economic Crime Centre[2] the threat from fraud, particularly scams, has never been greater. Fraud has increased nearly 36%[3], and now costs businesses and individuals across the UK £137 billion every year[4]. The cost of fraud to government institutions is also estimated at somewhere between £29 - £52 billion each year[5]. According to UK Finance[6], fraudsters are focussing their activity on authorised push payment (APP) fraud, where the consumer is tricked into authorising a payment to an account controlled by a criminal. The advanced use of this social behavioural engineering by fraudsters, means that victims are manipulated into being complicit, making it difficult for organisations to identify and prevent fraud. Sadly, it is also often difficult for victims to admit to behavioural manipulation, because they feel betrayed, so

[1] Amazon releases its first Brand Protection Report (aboutamazon.com)
[2] https://nationalcrimeagency.gov.uk/news/fraudsters-targeted-in-new-national-law-enforcement-campaign
[3] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2021
[4] https://www.crowe.com/uk/insights/financial-cost-fraud-data-2021
[5] https://www.gov.uk/government/groups/counter-fraud-standards-and-profession
[6] https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf

such activity increases the pain felt by victims and also makes it less likely that victims feel confident to report to a person that they have been influenced[7]. Amazon has developed tools to assist customers, including, a new self-reporting tool for fraud. We explain other actions we are taking below in more detail.

Question 1: Please can you outline the types of activity related to fraud that you see on your platforms and how this has evolved? Have your methods for preventing fraud changed over time, what is the process by which users report fraudulent activity and what steps do you take when it is reported?

We take combatting fraud extremely seriously, whether it directly occurs on our website, or whether bad actors use the Amazon name to commit customer support scams on UK citizens. We work hard to prevent frauds and scams from reaching our customers and to raise awareness and empower our customers to recognise fraudulent attacks that may reach them, so they can protect themselves. We are constantly on the lookout for new iterations of fraud, and continually invest in new tools to protect our customers.

Types of fraud

There are many types of fraudulent activity online, which are not unique to Amazon. Indeed, the types of fraud we experience in our UK business are consistent with those reported for the UK generally and include those referenced below which appear most relevant to your inquiry:

- Customer support scams: Customers are contacted by bad actors illegally using our name and pretending to be from Amazon. This type of fraud is experienced by many organisations from recent HMRC & Post Office scams to anti-virus and financial services scams hitting most major banks. When our name is used, these occur off our site and our internal controls cannot help identify or track them. However, as they impact our customers directly and indeed our brand, we make considerable efforts (outlined below) to support and provide potential victims with multiple channels to report the fraud to us so that reports to law enforcement can be made.
- Advertising fraud: This can take the form of malvertising (advertising that includes fraud or malware) and click-through frauds or adverts that deceive as to their purpose.
- Seller & Buyer Fraud: Where sellers claim to ship products but don't or fraudsters pretend to not receive goods. Aside from our robust mechanisms to prevent these, Amazon provides an A-z guarantee[8]. We launched the A-to-z Guarantee more than 20 years ago to protect customers who buy items that are sold and fulfilled, even by third-party sellers.
- Counterfeiting: is a distinct type of activity to fraud and is based on intellectual property violations. However, Amazon takes it extremely seriously and we have built robust proactive controls to protect customers, using a combination of advanced machine learning capabilities

[7] https://www.agingcare.com/Articles/Steps-to-Take-After-Falling-for-a-Scam-187073.htm
[8] https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=GQ37ZCNECJKTFYQV

and expert human investigators. We have developed powerful, industry-leading tools - including Brand Registry, Project Zero, and Transparency (detailed in the Brand Protection Report) - for brands to partner with us to ensure only authentic products are sold in our store.

Fraud over time

As UK Finance[9] report, social engineering, in which criminals groom and manipulate people into divulging personal or financial details or transferring money, is one of the increasing key drivers of fraud losses in recent times. Criminals have expanded their use of scam phone calls, text messages and emails, as well as fake websites and more than ever, social media posts, to trick people into handing over personal details and passwords. This information is used to target victims and convince them to make payments to the criminal. This has led to a significant rise in investment scams, which, according to UK Finance, are heavily enabled by fraudulent advertising, search engines and social media. In order to support the FCA in managing this vector of fraud, Amazon voluntarily implemented enhancements to our Policies, so that all financial advertisers are required to be on the FCA Authorisation list.

Amazon knows that bad actors will not stop trying to deceive customers and we invest and innovate to stay ahead. For example, in 2020 we spent $700 million worldwide, to help protect our stores from fraud and abuse. This is an increase on 2019 when we invested over $500 million. An example of a recent initiative, we are developing and piloting new mechanisms to assist customers and sellers to protect themselves from phishing scams. We developed a new customer self-service reporting tool for scams that not only simplifies the process, but also means that victims do not have to acknowledge their potential discomfort to a person, but can register remotely (we did this even though these fraudsters are only pretending to be from Amazon). We use that data to enhance our capability to identify and address the typologies used by fraudsters, for example looking at malicious telephone numbers being used by scammers, which has a great potential to reduce exposure to potential victims and we work closely with Law Enforcement to address our customer's concerns.

We are also committed to raising the awareness of customers to empower them. In addition to our in-depth and pragmatic customer and seller awareness guides[10] , we recently launched a targeted email awareness raising campaign to several million customers to raise awareness of the risks, while developing an awareness-raising interactive quiz to provide pragmatic counter-fraud advice to SMEs.

One other aspect of abuse against our customers that is developing over time, relates to the sophisticated industry that has developed in recent years, with numerous 'review brokers' looking to profit from generating biased reviews, by offering, procuring, selling, or hosting public and private groups where 'fake' reviews are exchanged for compensation. Amazon believes that customer reviews play an important role in driving good consumer and competition outcomes. They help customers to make informed choices, enable businesses to receive feedback and innovate to improve products/services and enable SMEs to grow an audience and scale drive competition. To help earn the trust of our

[9] https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf
[10] https://www.amazon.com/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=G4YFYCCNUSENA23B

customers, Amazon devotes significant resources to preventing fake or incentivised reviews from appearing in our store and we go into further detail under Question 4 below. Effectively tackling the challenges brought by this harmful industry requires the cooperation of private entities, governments, law enforcement, consumer protection regulators, and consumer associations, towards a common goal of eradicating this industry.

How Amazon tackles fraud & counterfeiting

We have previously highlighted some of our targeted methods for protecting our customers from fraud and these focus on preventative action to stop fraud and abuse before it ever affects a customer or selling partner.

For example, we apply multiple mechanisms to detect and escalate fraud and abuse to a human investigator, depending on the situation. We have algorithms that look for abnormal activity on a seller's account or communications (a methodology for conducting the seller fraud referenced above). We apply (as relevant) natural language processing and IP geo-locators, to identify potential account take-overs (for example, where a seller's account is taken over by a phishing attack). We also use behavioural metrics, such as clickstream analysis to identify time spent on pages and velocity of sign-ins to identify malicious bots or abnormal activity. For a fraudster to monetise their frauds, they often need to change basic details, such as bank details or address details. We analyse over 5 billion changes daily to detail pages for signs of potential abuse. However, we also look at communication channels to look for signals of complaints or abuse and worldwide we blocked more than 4 billion bad listings before they were listed in our store. These listings were suspected of being fraudulent, infringing, counterfeit or at risk of other forms of abuse.

Backstopping this technology are 10,000 people focusing on protecting customers and our sellers globally. These dedicated teams are engaged in developing the machine learning algorithms, training them to recognise new fraud methodologies, reviewing the fraud alerts that the machines raise and collecting & investigating evidence which is passed to law enforcement. Just two examples:

- Amazon's Customer Protection and Enforcement team (CPE) specifically investigates fraudulent schemes that target customers, sellers and partners. They seek to identify and act against the bad actors behind them, so that proactive referrals can be made to law enforcement for onward action.
- Relating to counterfeits, in 2020 Amazon launched the Counterfeit Crimes Unit (CCU), a global team dedicated to working through the court system, and in partnership with law enforcement worldwide, to pursue counterfeiters and hold them accountable to the fullest extent of the law. Across its inaugural year in 2020, the CCU reported all confirmed counterfeiters that we had blocked from our store to law enforcement authorities in the U.S., the UK, the EU, Canada and China. For more than 250 counterfeiters, the CCU has taken the additional step of providing in-depth referrals and evidence to each counterfeiter's national authorities. The CCU also filed civil litigation against 64 counterfeiters WW, and disrupted counterfeiters and their supply networks through civil suits (including discovery) and joint enforcement actions and seizures with law

enforcement around the world, including against distributors, suppliers, logistics providers, and fake invoice providers.

Amazon believes that fraudulent activity is not a problem that any one company can solve on its own. It requires Government, law enforcement, private sector and civil society to work together in partnership, and to collaborate on joint initiatives. We are already working with others, in particular with the Home Office, DCMS, the tech industry and UK banks, and the Police Intellectual Property Crime Unit (PIPCU) department at the City of London Police, with the aim to make the UK the least attractive place for fraudsters to operate. Amazon has numerous partnerships worldwide and is also working to develop further partnerships.

The customer matters

Fraudsters rapidly develop new and sophisticated methods to counter robust mechanisms that organisations use to protect consumers. Therefore, in case any fraudulent or counterfeit activity slips through the net, we offer consumers redress through the A-to-z Guarantee.

An essential complement to Government and industry efforts is better public awareness. We work to educate our own customers, but also work in collaboration with others, such as our announcement last year to work with four other companies to provide $1 million to Take Five to Stop Fraud – a national advertising campaign that offers impartial advice to help people protect themselves. We are also working with Action Fraud to develop an awareness raising interactive fun Quiz for SMEs. There is a dearth of guidance specifically designed and developed to assist SMEs (who face unique challenges e.g. closer connection between home computers and work, unlikely to have fraud experts etc) and our plan is to develop pragmatic and practical advice delivered in a fun interactive medium.

Third Party sellers

Amazon has built industry-leading tools to verify potential sellers' identities. Our proprietary systems analyse hundreds of unique data points to verify the information and detect potential risk. Prospective selling partners are required to provide a government-issued photo ID and information about their identity, location, taxpayer information, bank account, credit card, and more. Our systems analyse hundreds of unique data points to verify the information and detect potential risk. Our verification processes stopped over 6 million attempts to create a selling account before they were able to publish a single listing for sale. For example, we match information against third-party or government records, such as verifying taxpayer identification numbers against tax authority records and work with payment service providers to identify where funds are disbursed and who the recipient is to make it harder for bad actors to mask their identity.

Results

As set out above, our verification processes stopped over 6 million attempts to create a selling account before they were able to publish a single listing for sale. This is a significant increase from the 2.5 million attempts we stopped in 2019, and it was driven by increased bad actor attempts to get into our store that we successfully thwarted, while only 6% of seller account registrations passed our robust verification processes and listed products. In 2020, we blocked more than 10 billion suspected bad listings before they were published in our store. We seized more than 2 million products that were sent to our fulfilment centres that we detected as counterfeit before being sent to a customer.

With regard to reviews abuse, we are committed to proactively prevent fake reviews from ever being seen in our store. In 2020, over 200 million reviews were either blocked or removed. More than 99% of reviews enforcement was driven by our proactive detection. We also banned over 1.2 million accounts in 2020 for suspected fake reviews and have sued multiple review brokers (and, where appropriate, reported them to law enforcement).

Question 2: What is your assessment of the Government's Online Advertising Programme consultation? What would you like to see in the Government's response to the consultation?

Amazon serves ads to customers on first-party properties (e.g. amazon.com, imdb.com) and third-party properties (e.g. www.nytimes.com). The Amazon Store helps selling partners reach UK consumers and amplify their offer. Ads through Amazon Ads is just one way that selling partners are able to increase sales of their products, increase brand awareness, and drive brand loyalty.

We recognize that advertising has changed over the past few years. The Government highlights that the Online Advertising Programme will work in conjunction with other live policy and legislative developments, such as the Online Safety Bill and the upcoming Media Bill. We are supportive for the Programme to co-ordinate with other policy agendas and ensure they complement each other; rather than creating uncertainty or potential overlap.

We believe an effective advertising framework should specifically distinguish between types of business advertising models and, explicitly in definitions and focus, provide clarity as to which initiatives are targeted at which types of business models. Overall, we believe that there are already existing mechanisms to protect customers from harm across the entirety of the supply chain and a more detailed mapping of the existing regulators and oversight bodies in this space would highlight the capabilities.

Going beyond the OAP

As highlighted by the Online Fraud Steering Group, Advertising Sub-Group[11] (a public-private group chaired by the NCA focused on reducing the threat from online/cyber enabled-fraud in the UK[12]), there is insufficient evidence of the level of advertising fraud leading to difficulty in targeting initiatives to where they can

[11] https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre?highlight=WyJuZWNjIiwibmVjYydzIl0=
[12] https://www.techuk.org/resource/online-fraud-steering-group-techuk-uk-finance-the-necc-collective-efforts-to-combat-fraud.html

do most good. Therefore, Amazon supports greater research in this area and have offered to collaborate with other companies and NCSC.

The key issue is where fraud is put into the system, not where it is targeted at people. Amazon would draw attention to the international aspect of the issue. In our experience, the majority of advertising harms described are caused by international attacks. It is therefore crucial that UK regulatory action can work hand in hand with international initiatives that are already underway (such as the information sharing initiatives in the Trustworthy Accountability Group[13]).

Question 3: What is your response to the fraud measures in the Online Safety Bill? We have heard calls for all platforms that host advertisers, regardless of size or type, to be treated equally with respect to the need to prevent fraud. What is your view?

Amazon has worked closely with the Government on the Online Safety Bill. It is in the interests of customers and regulated firms that the Bill succeeds in creating a proportionate, targeted regime that helps to address harmful content and retain customer trust in online content and services.

As proposed, the regime will apply to a very wide range of content, and will regulate a very large number of diverse businesses (estimated to be over 20,000). Whilst commentary around the regime often focusses on large social media firms, Amazon is an example of the diversity of business models that will be regulated. This includes retailers whose business model is based around selling goods and services to paying end customers, rather than seeking to monetise user-generated content.

Given the breadth and diversity of the regime's scope, it's crucial it is well targeted and flexible. We welcome the fact the regime is flexible in how it applies to different business models, recognising that risk will vary significantly across different businesses. It is also welcome that the regime predominantly focusses on defining what is expected, but leaves some discretion over how that is practically achieved across different firms. That enables firms to take a very tailored approach, building on their existing processes and technology in a way that is quick, effective and efficient, rather than seeking blunter, one-size-fits-all-solutions across very different businesses.

Fraud is agile, sophisticated, and changes constantly; and the response needs to be equally so. As a new fraud occurs, companies and law enforcement need to be able to adapt and update their machine learning templates in order to counter it and they need to be as agile as the fraudsters, who will design innovative solutions to circumvent any controls or processes required in new legislation.

The challenge, we believe, is one of enforcement and bringing bad actors to Courts and there is a need for better and more effective partnerships between industry, third sector and enforcement authorities and we are keen to play a constructive role. We think this will help deliver results in a more timely and beneficial way than adding new fraud-related requirements to the Online Safety Bill.

[13] https://www.isao.org/information-sharing-group/sector/trustworthy-accountability-group-tag/

One such partnership that we are proud to support is the Online Fraud Steering Group (for which we fund the secretariat), which brings together senior representatives from the tech sector, financial services and law enforcement to collaborate and take collective action to disrupt fraudsters. The Group has already enhanced awareness to consumers through a $1 million donation to Action Fraud and developed consistent Policy positions to support the FCA in targeting investment fraud.

Question 4: What can be done to better protect consumers against fake reviews potentially being used to sell fraudulent, counterfeit, or fake goods online?

Amazon customers tell us that product reviews are one of the most useful features in our stores and a key reason why they enjoy shopping at Amazon. Reviews give customers the confidence to buy or not buy a product, and reviews also provide a way for honest entrepreneurs to differentiate their products from similar items. But reviews are only beneficial if they accurately reflect people's real experiences with a product. In general, solicited 'fake' reviews are those generated through monetary or other incentives that do not reflect an impartial opinion of the good or service being reviewed. Amazon has clear policies that prohibit reviews abuse, including paying for reviewing and soliciting only positive reviews.

In contrast, review brokers are fraudsters who created an industry focused on posting fake and inauthentic reviews at scale. The brokers approach customers through their own websites and solicit them to write misleading or inflated reviews in exchange for money, free products, or other incentives. For example, Extreme Rebate ran fraudulent schemes that provided free products and paid members up to $4 per review for five-star reviews that are at least 15 words long and include pictures or videos. Earlier this year, Amazon took legal actions against three major fake review brokers—Fivestar Marketing, Matronex, and AppSally. The brokers have now stopped their fraudulent schemes targeting Amazon customers in the U.S., UK, Germany, France, Italy, and Spain. As a result, nearly 350,000 people using their websites and willing to write fake and misleading product reviews are no longer incentivised to do so. This is just one example from actions taken in the UK and worldwide[14].

We support the Government's desire to protect customers' freedom to leave accurate reviews, whilst tackling those that seek to mislead. This is not an area where a one-size-fits-all approach is in the best interest of consumers. We believe the best way the Government can do this is by:

- Accurately defining what fake reviews means. Focussing on 'fake' reviews, as the concept and capability to identify something as 'genuine' is complex, ambiguous and not scalable. The introduction of concepts such as 'genuine' is difficult to operationalise as it's not possible for a trader to analyse the substance of a specific review to determine accurately if it is authentic or genuine without risking to over-censor the consumer views and infringing on their freedom to express views, good or bad. This is certainly the case where 'genuine' has not been defined and the introduction of such a definition is likely to result in legal uncertainty and

[14] Fake Amazon review ring shut down by High Court in legal first (telegraph.co.uk)

fragmentation. By way of example of the likely difficulties these concepts may introduce, a trader will not be able to determine whether a consumer's review is honest and sincere (one aspect of the term 'genuine'). Consumers have individual specific perspectives on a product, and this is what makes reviews valuable to other consumers, getting feedback from consumers like them who have interacted with the product. As long as the reviews are submitted by actual consumers that were not incentivised through undisclosed monetary or other incentives, there is an overall benefit for other consumers to be able to experience the positive and negative feedback, from different angles and personal views.

- Prohibiting the commercial practice of incentivising 'fake consumer reviews' without prohibiting the broader commissioning or incentivising of consumer reviews in all circumstances. Commissioned reviews are not necessarily all fake. For example, a business may provide a consumer with a free new product or a small incentive in order to get the consumer's opinion of the product, which in turn is informative to both the business and other consumers. Without such commissioned reviews, it would be difficult for new businesses and products to find an audience, as consumers may be hesitant to purchase products without reviews. We believe that in such cases, it should be clearly disclosed that the consumer was incentivised to write the review; businesses should also not specifically ask consumers to write a certain type of review as a condition of accepting the incentive.
- Requiring businesses to take 'reasonable and proportionate' steps to prevent abusive reviews, which we believe are:
    - Creating and maintaining clear policies that define and prohibit fake reviews for products and services. The policies should clearly set out the actions that will be taken where non-genuine reviews are found to have been posted.
    - Providing mechanisms for consumers and third parties to report "fake" reviews to the business.
    - Collaborating with governments, law enforcement, consumer protection regulators and consumer associations to identify and pursue the bad actors in the "fake" reviews industry.
    - Exercising due diligence to proactively block or remove "fake" reviews on products and services.

Question 5: How would you respond to the potential introduction of a 'failure to prevent fraud' duty being introduced to incentivise action within companies whose platforms are used to facilitate it?

A 'failure to prevent' strict liability law is a legal doctrine often designed to focus corporate attention on developing pragmatic policies, processes & systems. Amazon is already well-motivated to protect its customers, eliminate fraudsters from its stores and even from wider society where those criminals use the Amazon brand to dupe victims into frauds.

Amazon always starts with the customer and launched the A-to-z Guarantee to protect customers. The Amazon A-to-z Guarantee between January 2020 to September 2021, responded to claims for over 190,000 customers due to potential or suspected fraudulent activity. The sums paid were over £1.5 million.

However, we go further and have already developed robust mechanisms to detect and prevent abuse on our stores. We have provided a number of examples above to demonstrate how we leverage a combination of advanced machine learning capabilities and expert human investigators to protect our store proactively from bad actors and bad products. We are constantly innovating to stay ahead of bad actors and their attempts to circumvent our controls and this includes:

- our industry-leading tools to verify potential sellers' identities through machine learning technology and expert human review
- our Payment Service Provider Programme where we work with payment service providers to identify where funds are disbursed and who the recipient is to make it harder for bad actors to mask their identity
- our scanning tools that scanned more than 5 billion attempted changes to product detail pages daily for signs of potential abuse
- our global enforcement teams, such as the CCU and Amazon's Customer Protection and Enforcement (CPE) team (referenced above).

Question 6: If you could suggest one policy recommendation to the Government, what would it be?

We have a number of recommendations and have made them under specific topics throughout this response (for example, the need for collaborative efforts to address the challenges from review brokers).

Amazon believes that the current UK regulatory framework, such as the Fraud Act or anti-counterfeiting IP protection, is effective and helps deliver results against bad actors. We would recommend that Government focusses on further supporting collaborative partnerships, such as the Online Fraud Steering Group to operationalise and use such capability better. For example, we know that driving counterfeits to zero is a global challenge that requires enhanced partnerships across industry and governments around the world. To better find and hold counterfeiters accountable, Amazon supports ongoing collaborations and expanded partnerships such as:

- Information exchange on counterfeit activity to help stop counterfeit products at the border
- Sharing information about blocked counterfeiters to help the industry stop more counterfeiters earlier

In conclusion, we are grateful for the opportunity to assist the Committee and begin to demonstrate Amazon's focus, resourcing and commitment to protecting our customers from fraud and abuse. It is our firm belief that fraud can only be tackled on a national scale through collaboration between the public and private sector and we are working on developing a number of initiatives to face the challenges that all citizens face.

7 June 2022