THREE STRIKES AND OUT

How e-commerce platforms can protect consumers from repeat offenders
E-commerce marketplaces and social media platforms are now essential sources for goods and services and brand owners must do what they can to protect themselves and their consumers from “bad actors” online, who misuse their brands to sell fake, sub-standard and harmful products and services that de-fraud and deceive.

Incopro supports many of the world’s largest brands – using technology to scan the internet to find and remove harmful products and services.

The challenge is ever increasing and so it is essential to ask whether more can be done. This is an urgent question for legislators and regulators in both the United States and the European Union.

Two initiatives being considered centre around improving verification of identity before sellers can list products or services for sale; and blocking sellers who repeatedly use e-commerce platforms to sell products and services that are fake or fraudulent.

Incopro has undertaken a statistical review of a sample of its enforcement data, covering over 1.5m non-genuine listings removed from online platforms between November 2019 and November 2020 - to assess the proportion of issues that Incopro has found online and removed that have been offered by the same seller on the same e-commerce marketplace or social media site.

The data shows that the proportion of sellers who most aggressively repeatedly use e-commerce operations to infringe rights and harm consumers typically comprises under 3% of sellers enforced, but these sellers are responsible for a disproportionately large number of the challenges that Incopro’s technology finds and removes – on average, over 20% of the identified illicit issues detected and notified on the e-commerce operations considered in this study.

The benefits of a consistently implemented verification and removal policy would be hugely significant. A minimum of 11% of all harmful online offers could be stopped immediately if these policies were implemented, and this rises to 24% if the removal policy were applied more strictly.

With this policy, consumers would be exposed to up to 24% fewer non-genuine offers on e-commerce platforms and social media sites. With online losses suffered due to online counterfeiting alone estimated at $323bn, this would mean at least $35bn saved by the more lenient policy proposals, and $78bn under stricter policies – with equivalent revenue captured by the true rights holders selling genuine products and services.

Aside from protecting consumers from harmful products or fraudulent listings, these policy changes would also reduce the burden of managing bad actors for platforms. Additionally, given research suggests 33% of consumers hold e-commerce operations responsible for addressing these issues, and 64% of consumers have lost trust in a platform after unintentionally buying counterfeit products on that platform, addressing this issue effectively is also likely to drive the commercial success of ecommerce marketplaces.

As legislators focus their attentions on this issue, and as platforms and brands attempt to deal with the threats to consumers posed by bad actors, there is a clear opportunity to drive improvements for all with policy changes focused on seller verification and removal.

1 The Global Anticounterfeiting Report, 2018 https://www.researchandmarkets.com/research/hzjb9c/global_brand?w=4
Incopro’s technology discovers brand misuse online. This can range from individual sellers on marketplaces offering fake products for sale through to sophisticated networks of individuals using a diverse social media presence to deceive and defraud consumers into giving away their personal data or transacting for fake or inferior products and services. These instances of brand abuse are referred to in this paper as “Breaches”.

**Incopro’s Technology Finds Repeated Breaches**

**Consumer Protection Legislation Not Working**

**Sale of Fakes and Fraudulent Services and Products That Breach Consumer Protection Legislation**
Incopro discovers and notifies thousands of Breaches every day. Once a Breach is discovered by Incopro’s technology, an automated notification is sent to the relevant e-Commerce operation, so that the Breach is removed.

For this paper, Incopro has focused on a sample of the data collated by its technology concerning Breaches by users of key e-commerce marketplaces and social media platforms (referred to in this paper collectively as “e-commerce operators”). This dataset contains over 1.5m listings that were removed by Incopro between November 2019 and November 2020.
The following is an example of what can occur in the absence of a strict platform response.

In the course of 2020, a seller used the same e-commerce operation in Latin America to offer consumer goods for sale. In total, Breaches in respect of 9 different consumer brands were found by Incopro’s technology. On each occasion, Incopro’s technology notified the e-commerce operation of the Breach and the seller’s online identification. The e-commerce operation was asked to remove the offer for sale. Over the course of a year, 107 different Breaches were identified. On one day, 27 separate Breaches that each offered a fake or inferior product for sale were reported to the e-commerce operation.

This bar chart (Figure 1) identifies the time period for the Breaches and notifications to the e-commerce operation.
Although this e-commerce operation was notified about the same seller on 27 separate days, this seller was not stopped from using the platform to create further offers for sale – the seller was free to continue to offer goods for sale that might place consumers at risk.

This example is not exceptional. As this paper shows, there are a relatively small proportion of people who use e-commerce operations to repeatedly undertake Breaches (typically around 3% of the data set), but they are responsible for a disproportionately large share of the overall problem (on average 20% of the Breaches in the data set).
Whilst the above example is not exceptional, it is increasingly clear that more needs to be done to stop those who are determined to misuse e-commerce operations to infringe rights and harm consumers. This is particularly so where consumers increasingly use e-commerce operators to buy products and secure services.

In its ‘Online Nation’ Report, OFCOM reported that 87% of people aged 16+ used the internet in 2019, with four fifths of their time online being through mobile devices. The Report also showed that major online operators continue to make up the majority of time spent online, with more than a third of measured time online being spent at locations owned by Google or Facebook.

E-commerce is the fastest growing segment of the retail market in Europe and in North America. As the global Covid-19 pandemic has continued, e-commerce has been “super-charged”. According to the Centre for Retail Research, combined e-commerce sales in Western Europe (UK, Germany, France, Netherlands, Italy and Spain) were £152.2 Bn in 2015 and reached £224.4Bn in 2019, an increase of 47.5%. By 2020, this figure had risen again to £294.2 Bn against a forecast of £249 Bn, representing growth of more than 31% in a single year.

E-commerce growth in the US increased by more than 30% in 2020, accelerating the shift to online retail by nearly two years. According to findings from eMarketer, US based sales from ecommerce in 2020 were approximately $794.5 Bn USD, an increase of 32% year-on-year.

In addition to this, ecommerce marketplaces have captured an outsized share of growth in online retail, with Forrester estimating that 82% of global B2C ecommerce growth came from marketplaces – demonstrating the importance of effective consumer protection on these channels.

And as e-commerce continues to grow, it is also estimated that the global economic value of counterfeiting and piracy could reach $4.2 trillion USD by 2022 placing 5.4 million legitimate jobs at risk over that period.

The Organisation for Economic Cooperation and Development (the “OECD”) is an intergovernmental economic organisation founded in Paris in 1961 to stimulate economic progress and world trade. The OECD estimates that trade in fake goods (as of March 2019) is 3.3% of global trade and rising.

In June 2020, the European Union Intellectual Property Office (“EUIPO”) published its “Status Report on IPR Infringement”. This report notes that in April 2016, the EUIPO working jointly with the OECD estimated that the extent of counterfeit goods in global trade was estimated to have reached as much as $461 billion by 2013. This study was updated in 2019 and the problem was estimated to have increased to $509 billion.

The Status Report notes the individual sectoral studies that the EUIPO has undertaken and notes that the sales decrease attributable to counterfeiting will vary by sector (from 1.6% for recorded music to 14% for cosmetics and personal care products) but that the estimated direct and indirect sales losses attributable to counterfeiting amount to EUR 83 billion each year. The report also notes the significant health and safety consequences of many counterfeit goods.

The Global Brand Counterfeiting Report, 2018 estimates that the amount of counterfeiting globally had reached $12 Trillion by 2019 and that the losses suffered from online counterfeiting amounted to $323 Billion in 2017.

Recognising that consumer harm and economic loss from brand misuse is an increasing threat as e-commerce continues to grow, legislators in the United States and European Union have tabled potential legislation aimed at helping brand owners and others to secure greater protection for their products and services online. A summary of the legislation under consideration is included at Annex A.
87% of people aged 16+ used the internet in 2019, with four fifths of their time online being through mobile device.

Third of time online spent at locations owned by Google or Facebook.

E-COMMERCE SALES IN WESTERN EUROPE

- £294.2bn in 2020
- £224.4bn in 2019
- £152.2bn in 2015

Losses suffered from online counterfeiting amounted to $323bn in 2017.

Counterfeiting and piracy may reach $4.2 trillion USD by 2022, placing 5.4m legitimate jobs at risk.

Trade in fake goods is approx. 3.3% of global trade and rising at March '19.
In this White Paper, “Repeat Breachers” are individual e-commerce users/sellers who have repeatedly used e-commerce marketplaces and social media platforms to offer for sale illicit goods or services that are either counterfeit and/or otherwise infringe trademark or copyright and/or otherwise breach platform policy or consumer protection regulation. Each type of Breach is important – it is essential to recognise that “bad actors” undermine brands whenever they sell fake products, but they also cause significant harm and loss (whether to the consumer, business or taxpayer) whenever they offer sub-standard or un-licensed products and services and whenever they breach consumer protection legislation. Incopro’s data for this paper deliberately includes all of the harms that Incopro has identified and that e-commerce operations have removed over the course of a year and not just those that are purely “counterfeit” harms.

“Bad Actor” e-commerce users/sellers have been identified by Incopro and a notification has been sent to the relevant e-commerce operation asking that the offer for sale or listing be removed. Incopro’s request has been acted on by the e-commerce operation concerned - by removing the particular offer for sale or service that Incopro has identified. The same seller, using the same seller identification has also created another offer for sale or listing – either for the same item or service or for a different one.

The methodology employed in this White Paper to identify and assess the proportion of Repeat Breachers is set out at Annex B.

When considering Incopro’s data on Repeat Breaches, it is important to point out that those who use e-commerce operations to undertake repeated Breaches know that they are selling goods or services that are counterfeit or otherwise in breach of intellectual property law and/or consumer protection/platform regulation. When a notice of infringement is sent to an e-commerce operation, the seller concerned is contacted. As such, that seller is aware that he or she has been selling products or services that he or she should not be selling.

Incopro has analyzed the effect that further action by e-commerce operations might have if these operations implemented a robust verification policy and stopped sellers based on two potential policy revisions. Firstly, the potential impact if sellers were banned from platforms following enforcements on their listings over three separate days, and secondly, if sellers were banned following enforcements on three separate listings.

OUR ANALYSIS

In this White Paper, “Repeat Breachers” are individual e-commerce users/sellers who have repeatedly used e-commerce marketplaces and social media platforms to offer for sale illicit goods or services that are either counterfeit and/or otherwise infringe trademark or copyright and/or otherwise breach platform policy or consumer protection regulation. Each type of Breach is important – it is essential to recognise that “bad actors” undermine brands whenever they sell fake products, but they also cause significant harm and loss (whether to the consumer, business or taxpayer) whenever they offer sub-standard or un-licensed products and services and whenever they breach consumer protection legislation. Incopro’s data for this paper deliberately includes all of the harms that Incopro has identified and that e-commerce operations have removed over the course of a year and not just those that are purely “counterfeit” harms.
Here, Incopro considers a scenario where the relevant e-commerce operation imposes a ban on a seller from advertising further products or services when enforcements against that seller have been sent on three separate days.

To model this, Incopro has taken the data for sellers enforced on 4 or more enforcement days and considered what would happen if these sellers were prevented from listing products once enforced on 3 separate days. The effect would be that these sellers would have been unable to list on the relevant e-commerce operation under the same name after 3 days of enforcement. All offers for sale or service made by the same seller after the 3rd day would not have taken place because, on this hypothesis, that seller would have been blocked by the e-commerce operation.

Figure 2 shows the sample data with users grouped by the number of separate days of enforcement – demonstrating that the most egregious Repeat Breachers who are enforced on 4 or more days represent on average less than 3% of users on a platform, and this proportion increases to only 6% when users enforced on 3 separate days are included.
However, whilst these users comprise a small percentage of the overall users in the data set, they are responsible for a significant proportion of listings as shown by Figure 3 – on average, 21% of Breaches on the platform in this study. However, there is significant variation by platform, with some platforms such as Facebook seeing almost no repeat offenders under this definition.

Implementing a model whereby Repeat Breachers were banned from a platform after three separate days of enforcement would deliver material reductions in the volume of infringing listings – 11% of all Breaches would never have been listed online under this model, as the user would already have been banned.
Figure 4 demonstrates the potential reduction in Breaches by platform – calculated by assessing the number of Breaches which were offered online following the point that the user would have been banned under this model. This shows that for 22 of the 34 platforms analysed, this policy change could reduce Breaches by at least 5%. 

![Figure 4: Reduction in Infringing Listings if Users Were Banned After 3 Separate Days of Enforcement](image-url)
Model 2: Threshold = 3 enforced listings

Here, Incopro considers a scenario where the relevant e-commerce operation blocks a seller from advertising further listings when a limit of 3 enforced listings is reached. To model this, Incopro’s data is grouped based on the number of separate listings that have been enforced.

For example, User A has 3 days of enforcement in total. On the first day he/she has 1 listing enforced against. On the second day of enforcement, 5 further items are enforced against. This enforcement behavior would trigger the platform to block User A because he or she has offered more than 3 enforced listings. As such, no further listings would be enforced against for this user. User A would be assigned to the 2 days of enforcement group. All the listings accrued up to this point, a total of 6, are counted as his/her listings. Subsequently, the listings that would have occurred on User A’s third day of enforcement are regarded as a saving as previously defined.
Under this model, the potential reduction in Breaches is significantly higher – 24%, as shown in Figure 5. This is because in many cases, the most active Repeat Breachers are responsible for multiple Breaches – and if at least three of these were enforced on one day, then they would be removed from the platform faster than under Model 1, leading to fewer Breaches ever making it online.

Whilst e-commerce operations have a broad range of considerations to consider when designing their policies, it is notable that 28 out of the 34 platforms in this study could reduce the volume of Breaches on their platform – protecting consumers and their trust in the platform by over 10% if this stricter model was implemented.

The Impact of the Savings
Implementing either of these policies could reduce the availability of potentially harmful or low quality, non-genuine products to consumers by a minimum of 11% (Model 1) or up to 24% (Model 2). Given the losses suffered to online counterfeiting are estimated at over $320bn annually, this could equate to consumer savings of $35bn under Model 1 and up to $78bn under Model 2.

However, the benefit is not just financial. Non-genuine listings and counterfeits are often low-quality products, or those that may not meet regulatory standards, and are therefore highly likely to pose risks to consumer health and safety. And given that 64% of consumers said they would lose trust in a platform after being deceived by a breach, there are clear benefits to platforms as well.

Under the assumption that the enforcement data included here are typical and noting that individual e-commerce operations vary, Incopro’s analysis shows that:

• Only 6% of sellers are repeatedly enforced on 3 days or more
• However, these sellers are responsible for over 24% of the listings Incopro has enforced against
• The models show that a seller verification and repeat infringer policy would benefit consumers, brands, legislators and the platforms themselves.

Non-genuine listings and counterfeits are often low-quality products, or those that may not meet regulatory standards, and are therefore highly likely to pose risks to consumer health and safety.
Given the positive benefits e-commerce operations can drive for both brands and consumers by tackling repeat Breaches, it is important to understand what platforms currently do. The platforms in the scope of this study were therefore considered and analysed in respect of three key areas:

1. Whether e-commerce operations analysed have a policy against repeat Breaches.
2. Whether the policy includes a 3-strike rule;
3. Whether the policy sets out the duration of the suspension.

Terms and conditions and other evidently available information sources such as an e-commerce operations’ help centre, policy centre, and seller centre were reviewed to answer these points, in addition to inviting input from the e-commerce operations considered in this study.

23 of the 34 e-commerce operations considered have a policy directed at repeated Breaches. The remaining 11 have no relevant policy evident.

Out of the 23 e-commerce operations that have a policy directed at repeat Breaches, 3 have a policy which includes a clear adherence to the 3-strike rule.

Regarding the duration of suspension, 10 out of 23 e-commerce operations with a relevant policy have published definitions of the penalty period. Amongst these 10 operations, 2 have a policy that considers repeat Breach a sufficient ground for immediate termination.

It is noticeable that platforms like Aliexpress, which has a clear ‘three strikes’ rule and robust seller verification process, sees fewer Repeat Breaches than other platforms. Similarly, whilst Facebook and Instagram prefer not to disclose their policies publicly (to avoid gaming by bad actors), we are aware that they pay close attention to the issue of Repeat Breaches – reflected in the strong performance in this analysis.

Incopro contacted the platforms reviewed in this study, and was pleased to see significant positive engagement and desire to address these issues; a full summary of responses is included in Annex D. A number of topics were covered in responses, including a desire to retain flexibility with respect to the type of Breach, a desire to distinguish between clear illegality and ‘inadvertent’ breaches, as well as the technological and capacity challenges in effectively addressing these threats. However, collaboration was highlighted as a consistent theme, and Incopro looks forward to working with the ecommerce operators to help protect consumers in the future.
Incopro’s analysis shows that significant business and consumer protection could be secured with the consistent implementation of robust verification of seller identity combined with strict removal for those that repeatedly offer products or services that are fake or otherwise misuse intellectual property or breach consumer and platform regulation. Implementing these policies could reduce the potential risk to consumers by up to 24% at a time when there has been vast acceleration in usage of ecommerce operations. Effective policy in this area would protect consumers, rights holders, and trust in the platforms themselves.

Incopro has greatly welcomed the dialogue and cooperation that it has had with many of the e-commerce operators referenced in this study. Incopro believes that a strategy of identification and enforcement directed at stopping repeated misuse of e-commerce operations is in the interests of brands, consumers and e-commerce providers - we welcome and look forward to continued engagement to secure the most effective methods to protect brands and consumers online.
ANNEXES
Annex A: A summary of the legislation under consideration in the US & EU

US LEGISLATION

SHOP SAFE Act
The Shop Safe Act was a bi-partisan Bill introduced on 2 March 2020 with the aim of "creating accountability to prevent hazardous items from infiltrating the homes of millions of Americans". The Bill is not currently before Congress for consideration, but it is widely expected to be re-introduced in some form. Its key features include:

- a codified set of 'best practices' on screening sellers and tackling repeat offenders in return for liability protection;
- a focus on goods with a health and safety component (goods which may give rise to illness/ disease/ injury/ serious adverse events/ allergic reactions or death);
- application to any e-commerce platform which sells to US consumers.

Trademark Modernization Act ("the TMA")
The TMA was enacted into law on 27 December 2020 with the aim of strengthening and improving the accuracy and integrity of the federal trademark register. Its key features include:

- improving US Trade Mark Office registry process and procedures including measures to improve consumer protection (including codification of a rebuttable presumption of irreparable harm in the event of a Court finding there has been an infringement given the consumer protection concerns which would arise otherwise).

INFORM Consumers Act
The Inform Consumers Act, introduced to the US Senate on 23 March 2021, has objectives similar to those under the Shop Safe Act, with a focus on transparency. It aims to require online marketplaces to collect and authenticate basic seller information which sellers must also provide to consumers. Its key features include:

- requiring online retail marketplaces which include third-party sellers of consumer products to authenticate the identity of "high-volume third-party sellers" through disclosure of seller information, government IDs, tax registration details, business address, telephone and email, etc.
- "high-volume third-party sellers" are defined as vendors who have made 200 or more discrete sales in a 12-month period amounting to $5,000 or more.
- a requirement that online marketplaces disclose to consumers in a clear and conspicuous manner on the product listing of any high volume third party seller a reporting mechanism that allowed for "electronic and telephonic reporting of suspicious marketplace activity" (such as the posting of suspected stolen, counterfeit, or dangerous products) to the online marketplace.

SANTA Act
The SANTA Act is another consumer protection orientated, bipartisan initiative focused on transparency. Its key features include:

- requiring marketplaces to display a seller’s full name, business address, telephone number and working email address;
- a requirement to notify buyers if the product shipped is supplied by a seller other than the one detailed in the product listing.

EUROPEAN UNION LEGISLATION

The Digital Services Act
The Digital Services Act package of measures (the "DSA"), published by the European Commission on 15 December 2020, represents (potentially) the most sweeping reform to regulation of the internet economy in Europe in close to two decades. Assuming the legislation is enacted into law, platforms will find themselves having to do much more from a brand and consumer protection perspective – and may face financial penalties if they do not. With the DSA, the European Commission is seeking to become the global leader on tech regulation, in much the same way it has with data privacy through the GDPR.

The DSA includes:

- A requirement that larger E-commerce platforms verify seller information to establish the true identity of the seller.
- A requirement for platforms to suspend for "a reasonable period of time" (and after having issued a prior warning), the provision of their services to recipients that frequently (repeatedly) provide manifestly illegal content. No guidance is given on what amounts to a "reasonable period of time".

11. Stopping Harmful Offenders on Platforms by Screening Against Fakes in Ecommerce…Act
12. US Republican Representative for Georgia’s 9th Congressional District, Douglas Collins.
13. Stopping All Nefarious Toys in America Act
Annex B: Data Analysis Methodology

Data Source and Collection
Retained data relating to Breaches identified by Incopro, notified to e-commerce operations and removed by those e-commerce operations was retrieved from Incopro’s database.

The data collated is referred to in this paper as “Incopro’s Enforcement Data.”

The data represents a sample of Incopro’s enforcement activities, and:

• was originally collated and stored by Incopro in the period between 1 November 2019 and 2 November 2020;
• identifies individual offers for sale or “listings” found on e-commerce operations that are monitored using Incopro’s brand protection technology;
• identifies an instance of enforcement in respect of such an offer for sale or listing.

The analysis of the Incopro Enforcement Data concentrated on specific fields:

• “actioned_at_time”: the date and time that a notification was sent to a particular e-commerce operation (as recorded by Incopro’s brand protection technology);
• “friendly_id”: a unique identifier for each listing discovered by Incopro’s technology (this ID is created by Incopro);
• “user_id”: an identifier that is typically allocated to an individual user/seller by an e-commerce operation and that is generally unique for a given user.

The analysis of the Incopro Enforcement Data undertaken in this White Paper required the identification of:

• each individual user by reference to that user’s user ID;
• the notified Breaches that relate to that user;
• the number of separate times and days that a Breach has been identified and a notification sent in respect of a listing created by that user/seller.

E-commerce operations operating in more than one territory using a different version of the same platform were grouped together so that the data relating to the whole of that E-Commerce Platform’s business was considered collectively.
The data was grouped according to the number of separate days that an enforcement had been sent to a platform concerning a particular user as identified by that user’s unique ID. In this analysis there are 4 distinct groups:

- Enforcement on 1 day,
- Enforcement on 2 days,
- Enforcement on 3 days and
- Enforcement on 4 or more days.

For example, if we take two users: user A and user B. User A’s listings might have been enforced against by Incopro on 4 distinct days and user B’s listings might have been enforced against on 2 distinct days. User A would be grouped in our 4 or more days grouping and User B in the 2 days grouping.

To limit the analysis to a meaningful set of results, all platforms with fewer than 100 users in total for the sum of all groupings greater than one day were discarded from the analysis. The remaining subset of e-commerce operations can be viewed therefore as the operations where Incopro has detected a significant number of infringements for users enforced against two times or more.

The results of this analysis for all the Significant Platforms analyzed in this study are summarized in Figures 6 and 7 (the same data as previous Figures 2 and 3). The bar chart is obtained by stacking and color coding the results for each platforms users and listings respectively. Here, the enforcements for the platforms studied are ranked by the proportion of users within each grouping (days 1 to 4+). The red part of the chart indicates the proportion of the users on each platform that have been the subject of an enforcement notice sent by Incopro on 4 or more days.

From these latter figures we see that, although results across platforms vary, the number of users with 4 or more repeat days of enforcement are generally relatively few when compared to users with those with 3 or less days as indicated by the blue, green and orange portions of the stacked bars.

However, from Figure 7 we see that this small number of users has a disproportionate effect when the numbers of enforced listings are taken into consideration.
FIGURE 6 SUMMARY OF USER RESULTS. THE RESULT OF GROUPING USERS BY THE NUMBER OF DISTINCT DAYS THAT EACH USER HAS BEEN THE SUBJECT OF ENFORCEMENT NOTICES: 1 DAY ONLY, 2 DAYS ONLY, 3 DAYS ONLY AND 4 OR MORE DAYS
FIGURE 7 SUMMARY OF LISTING RESULTS. THE RESULT SHOWS THE PERCENTAGE OF LISTINGS ASSOCIATED WITH THE USER GROUPINGS DISPLAYED IN FIGURE 1: 1 DAY ONLY, 2 DAYS ONLY, 3 DAYS ONLY AND 4 OR MORE DAYS
Model 1: Threshold = 3 separate days of enforcement.

Here, Incopro considers a scenario where the relevant ecommerce platform imposes a ban on a seller from advertising further products for sale using the e-commerce platform when a limit of 3 separate days of enforcement is reached.

To model this, Incopro has taken the data for sellers enforced against on 4 or more enforcement days and considered what would happen if these sellers were prevented from listing products once enforced against on 3 separate days. The effect would be that these sellers would have been unable to list under the same name after 3 days of enforcement.

For example, if User A had previously had listings enforced on 4 separate days he/she would now only have 3 days of listing enforcements – the fourth day of enforcements would not have appeared because Seller A would have been stopped from offering items for sale by the ecommerce platform.

If User B has 10 days of enforcement, he/she would only have 3 in this hypothetical scenario – because the relevant platform would have blocked User B after the 3rd day of enforcement and so listings 4 to 10 would not have appeared on the platform.

A consequence of this is that all the users are still accounted for in Incopro’s grouping process, but no users would appear after 3 days of enforcement. In effect the users in the 4 days or more group are now found in the 3 day group.

Note that this is not true for the listings enforced against after the users 3 days of enforcement. Enforcing against these listings would no longer be required. This would represent both a saving in terms of enforcement effort and would also mean that brands as well as consumers would be less exposed to counterfeit goods.

Figure 8 shows the effect assuming a threshold of 3 days enforcement on the users remaining on the platform, segmented by number of days enforced.

Once again referring to the example in Figure 5 we would expect to see that the proportion of users with 3 days’ worth of enforcements is now the sum of the 3 and the 4 days or more groups from Figure 5.

As explained above, the model does not change the number of users (the sum of each stacked bar = 1) it merely changes their distribution amongst the groups. However, the effect on the listings enforced is pronounced (Figure 9).
Figure 8 Summary of Remaining Users Following Application of Model 1 by Number of Days Enforced

Summary User Results: threshold = 3 days

Percentage of Total Users

Site Group

1 Day  2 Days  3 Days
Below, we see that the total sum of the proportions of listings enforced against does not equate to 1. The shortfall represents the saving in listings that would no longer be required to be enforced following the removal of Repeat Infringers after 3 days of enforcement. (Saving = 100 – the sum of stacked bars in Figure 9).
Here, Incopro considers a scenario where the relevant platform blocks a seller from advertising further listings when a limit of 3 enforced listings is reached. To model this, Incopro’s data is grouped based on the number of separate listings that have been enforced.

For example, User A has 3 days of enforcement in total. On the first day he/she has 1 listing enforced against. On the second day of enforcement, 5 further items are enforced against. This enforcement behavior would trigger the platform to block User A because he or she has offered more than 3 enforced listings. As such, no further listings would be enforced against for this user. User A would be assigned to the 2 days of enforcement group. All the listings accrued up to this point, a total of 6, are counted as his/her listings. Subsequently, the listings that would have occurred on User A’s third day of enforcement are regarded as a saving as previously defined.
Figures 10 and 11 show the effect of this model on our data. Once again, we see that the sellers are all accounted for in this model but are reassigned to groups depending on the rules (Figure 10). Also, similarly to Model 1 there is a shortfall in the number of listings accounted for and these are regarded as a saving (Figure 11). Note that the saving is considerably higher than that gained from Model 1 as sellers are more likely to trigger the threshold earlier. In addition, as we noted above, the implicit conclusion that the repeating offenders are more likely to list more items means that the effect is magnified in terms of savings.
FIGURE 11 REMAINING BREACHES ON PLATFORMS, GROUPED BY USERS AND NUMBER OF DAYS ENFORCE, FOLLOWING APPLICATION OF MODEL 2
Annex C: Examples

The following examples help to illustrate the impact that could be secured. In each case, a bar graph displays the effect. The range of values in the bar graphs below covers several orders of magnitude and for this reason we use a logarithmic scale (complaints with one listing are not represented) to show how enforcement action for the particular seller was spread over the year. Each bar represents enforcement on a separate day, with the height of the bar representing how many individual listings were the subject of enforcement on the day in question. Below the graph are 12 pie charts, each representing the cumulative action taken against the seller in question during the year.

KEY TO BAR GRAPHS:
GREEN = listings enforced before the cut-off point had been reached.
TEAL = listings enforced after the cut-off point had been reached.

For the “listing” graphs, the cut-off point is 3 enforced listings. However, all the listings on the day which included the 3rd listing are regarded as being before the cut-off. Following the day when 3 or more listings are enforced, all bars are Teal.

For the “day” graphs the cut-off point is 3 separate days of enforcement. From day 4 and onwards all bars are Teal.

KEY TO PIE CHARTS:
TEAL = the proportion of listings enforced for the year before a cut-off point had been reached.
BLUE = the proportion of listings enforced as a proportion of total enforcements for the year enforced after a cut-off point has been reached.
GREEN = listings which by the point of cut-off had not been enforced.
Japanese Marketplace

A seller used an e-commerce platform in Japan and created 2,063 separate listings under the same name for products copying the intellectual property of a fashion brand protected by Incopro. Incopro’s technology discovered these listings as they appeared over the course of the year. Each time listings were discovered, notices were sent to the e-commerce operation to remove the products. Notices were sent on 42 separate days over the course of the year. Each time, the notified listings were removed by the platform, but the seller was able to continue listing offers on that platform.

If the seller had been stopped from using the marketplace after 3 listings were reported and removed, at least 2,060 of the seller’s infringing listings would not have required enforcement (see Figure 12).
If the seller had been stopped from using the marketplace after 3 separate days when listings were reported and removed, at least 1,795 of the seller’s listings would not have required enforcement (see Figure 13).
A seller used an e-commerce operation in South East Asia to offer for sale counterfeit jerseys for many of the world's most recognized football teams. When Incopro’s technology identified listings appearing, a notice was sent to the e-commerce operation and the listings were removed. Altogether notices were sent for listings created by this seller on 72 separate days.

If the seller had been stopped from using the e-commerce operation after 3 listings were reported and removed, at least 200 of the seller's infringing listings would not have required enforcement (see Figure 14).
If the seller had been stopped from using the marketplace after 3 separate days when listings were reported and removed, at least 199 of the seller’s infringing listings would not have required enforcement. (see Figure 15).
A seller used several e-commerce operations in the US and Europe to offer for sale counterfeits of globally recognized luxury goods. When Incopro’s technology identified listings appearing, a notice was sent to the relevant platform and the listings were removed.

If the seller had been stopped from using the e-commerce operations concerned after 3 listings were reported and removed, at least 153 of the seller’s infringing listings would not have required enforcement. (see Figure 16).
If the seller had been stopped from using the e-commerce operations after 3 separate days when listings were reported and removed, the seller would have been stopped from using European marketplace platforms and would never have expanded activity to sell in North America (see Figure 17).
Incopro contacted key e-commerce operations relevant to this study to ask for comment. Not all e-commerce operations provided a response, but many engaged in constructive discussion with Incopro and the following section summarises the points made. Incopro welcomes the engagement and notes that there are many very good examples of best practice.

The purpose of this study is not to suggest that all e-commerce operations are failing to take measures to tackle repeat infringement. There is however, clear evidence that where seller verification and repeat Breach blocking are not uniformly implemented (and there are certainly considerable variances in approach between the practices employed by the e-commerce operations studied) the prevalence of repeat Breach activity is still proportionately high overall and there is clear statistical evidence that a uniform regulation in this area is likely to deliver meaningful progress as less robust e-commerce operations adopt the best practices employed by some.
Responses on the data in the study

A number of e-commerce operations have noted that the data in this White Paper does not specifically identify whether the Breaches that have led to removal of the particular offer for sale are in respect of counterfeit product or whether the Breaches relate to other factors. As such, these operations have stressed that the data in this report should not be considered as only relating to counterfeit products and should not be relied on to build policy directed solely at stopping counterfeit sales. Incopro has been clear in this study that its analysis concerns data relating to notifications sent to e-commerce operations where the notification has identified a Breach (which is defined to include, but not be limited to, counterfeit sales) and the e-commerce operation has taken steps to remove the product or service identified. This removal may have been because the offer for sale misused intellectual property or otherwise breached consumer or platform regulation. Incopro’s view is that consumer and business harm is not limited only to counterfeits and the fact that e-commerce operations have removed offers for other reasons suggests that most stakeholders should be able to agree that tackling repeat Breaches in the broadest sense is something to aspire to and regulate for.
Responses on seller verification and seller blocking

- Some e-commerce operations prefer to have flexibility to respond to different circumstances in different ways. For example, a seller trading in goods that may cause consumer harm may be subject to restrictions on trading faster than a seller misusing photographs to trade in products that are either not harmful or not counterfeit. Several noted that in appropriate circumstances, a seller can be blocked from making further sales after “one-strike”, rather than waiting for three notifications before addressing the issue. Incopro recognizes that some e-commerce operations are geared up to respond in a very bespoke and individual way. However, the overall evidence from the data in this study suggests that a uniform and “baseline” requirement on all e-commerce operations with regard to seller verification and seller removal for repeated Breach is likely to significantly reduce the overall scale of Breach taking place using e-commerce operations like the ones studied in this report.

- Some e-commerce operations have noted that strict policies around seller verification will not be appropriate in all cases and have argued that they are more suited to commercial-scale business sellers, rather than individual ‘C2C’ sellers (especially where a platform is focused on highly localized markets). Some noted that sellers may themselves be duped or defrauded into offering products or services that are Breaches and they should be given the opportunity to understand where they may have been misled. Furthermore, if suspension policies are overly broad, this may result in an impact to the online ecosystem and online economy. Some have suggested that to place strict verification on individual consumer sellers would stifle activity and would operate as a disincentive to honest, individual sellers. Incopro recognizes that different considerations may need to apply to consumer sellers, while noting that there is a balance to be struck to prevent bad actors accessing platforms without first being checked and to stop repeat Breaches occurring.

- Several e-commerce operations noted that any law requiring cessation of use of a platform needs to allow for a seller to adjust his or her behavior before that seller is subject to a sanction in the form of a block. The seller may need to be informed and educated about what can be sold and this would suggest that a repeat Breach cessation policy should allow time between each notification so that a seller can learn and adjust before any cessation of use is imposed. Incopro notes that the data suggests that a policy requiring removal for Breach identified and notified to the seller over 3 separate days would still result in a significant reduction (11%) in overall Breach for the e-commerce operations studied. As regards the “three strikes and out” model, one platform was stated to be in favor of policies which zero-in on individuals who deliberately misuse online services to break the law, noting that the key is being able to separate deliberate abusers from the majority of honest users who need education or may have made an honest mistake. Incopro notes that it is possible to identify the characteristics of those sellers and e-commerce users who are operating at commercial scale. Incopro’s technology enables brands to identify such operators to e-commerce operations wishing to tackle significant and business operated e-commerce users.

As we have reported in this paper, some e-commerce operations do have strict seller verification policies that assist in enabling brands to stop Breaches undertaken at a commercial scale. Matters considered by these platforms can include checking government-issued photo ID and other identity information as well as matching against available government records, such as verifying taxpayer identification numbers. One major e-commerce operation noted that verification extends to checking IP address and verifying that the seller registration is not bot generated and further checking that the seller has not previously been blocked from selling for prior Breaches. This platform also noted that it has started to display seller business names and addresses on
the platform so that platform users can know more clearly who they are trading with. Incopro fully recognizes the best practice policies pursued by some key e-commerce operations and the difference that can be seen in terms of the proportion of repeat Breach between e-commerce operations that adopt strict policy and those that are less robust. Incopro welcomes instances of best practice as a base position to be implemented by all major e-commerce operations.

• Some platforms have pointed to having repeat Breach policies that are either intentionally vague/lacking detail or which are withheld from publication completely (the logic being that if full details are published, Breachers will (armed with that information) find ways to circumvent them). Incopro recognizes the merit in this approach, while also noting that if a consistent approach were taken across all e-commerce operations, the problem would be less likely to arise in the first place.

• Some e-commerce operations have identified resource and technology constraints that make it hard to implement a uniform seller verification and blocking policy. Incopro accepts that some e-commerce operations are less well-funded but we note that the issue may be more one of prioritization of resources for some e-commerce operations where there may be an inadequate funding of the teams and technology required to tackle Breaches that harm business and consumers.

• Some e-commerce operations with issues around repeat infringement and scaled abuse have expressly recognized the importance of working together on this issue, on the basis that they don’t always possess the cross-platform, cross-regional insights which Incopro has, meaning they do not have a complete picture of the repeat infringement landscape. Platforms which operate on consumer-to-consumer model have been especially keen to emphasize the importance of collaboration (especially with brand owners and with brand protection experts). Sharing reliable data through collaboration ensures that those platforms are best placed to a predominantly deal with policy breaches and counterfeits. As one platform noted, the “Trusted Flagger” status anticipated by the Digital Services Act underscores the importance of collaboration – platforms who work with brands or their agents as “Trusted Flaggers” are more likely to be achieving favorable outcomes for brands and consumers.
Responses directed to broader initiatives aimed at curtailing Breaches

- Some e-commerce operations take a pro-active approach by attempting to detect Breach listings before they are allowed to feature on the relevant platform. Here, these operations welcome collaboration with brands and companies like Incopro to ensure that Breaches are correctly identified and also work with wider law enforcement to stop challenges at source. Incopro acknowledges and welcomes these examples of best practice and the positive role that collaboration between relevant stakeholders can play.
ABOUT INCOPRO

Incopro tracks and prevents brand misuse and consumer harm taking place online. Over 750 global brands use Incopro to protect their e-commerce revenue and online consumers.

Incopro has offices in the UK, USA & China. In 2018, the company secured $21m in Series A funding, backed by Highland Europe.

incoproip.com
incoproip.com/contact-us
London, Cardiff, Shanghai, Boise, Los Angeles