*This PRFAQ describes the final product launch with various capabilities, each of which will roll out in multiple incremental phases*

**Buy with Prime Launches Advanced Monitoring & Moderation Capabilities to Protect Customer Experience & Safety**

*Business Wire, Seattle QX 2023-* Today, Buy with Prime (BwP) announced launch of new monitoring & moderation capabilities to improve safety and security of Buy with Prime shopper and merchant experiences. The new monitoring & moderation capabilities leverage machine learning algorithms to automatically identify and flag potential cases of violations with regards to content on the site, Accepted Use Policy (AUP), Amazon/BwP trademark use and other types of violations.

These functionalities are designed to provide a safer and more enjoyable shopping experience for all customers. By proactively identifying and removing fraudulent or inappropriate content, Buy with Prime will ensure that shoppers can shop with confidence, leading to increased trust and loyalty. Jenny McPhee, a long time Buy with Prime shopper said, “I shop through Buy with Prime because when I see the Prime badge, it increases my confidence in making a purchase. If I saw the Buy with Prime badge on illegal or inappropriate products like products that represent hate speech, sexually explicit products, guns or ammo etc. it would devalue the Prime experience for me and make me think of the site as spammy since such products are not available on Amazon.com. With the launch of these new fraud busting capabilities, I can say that Buy with Prime is committed to shopper safety excellence.”

Apart from solving for default fraud mitigation scenarios like content or AUP violations, these functionalities can also be customized by Buy with Prime product teams for their own use-cases. “We were seeing a few cases of bad actors publishing unauthorized fake Reviews from Amazon (RFA) on their DTC sites”, said Ben Li, Product Lead of RFA, who used the newly launched capabilities, in beta phase, to flag bad actors. “I cannot tell you how simple it was for my team to use the monitoring & moderation capabilities. It was a seamless experience and took us less than an hour to onboard onto the platform, and register the checks we would like to run. Within the same day, we started to get results of URLs that had unauthorized use of RFA widgets. I was very impressed with accuracy of the search results and the less than 0.5% false positive rate.” These capabilities can also be used by broader Amazon teams to solve a host of issues. “The unauthorized use of Amazon Trademarks is strictly prohibited as it is a threat to brand reputation. In order to mitigate this threat on merchant DTC sites, my team signed up for the trial phase of monitoring & moderation functionalities,” said Eileen Kellar, Senior Counsel, Amazon Trademarks Team. “What really stood out, apart from the quick onboarding, automation, and performance metrics was the Fraud Risk Investigations Team, who provided a swift and robust layer of human intelligence to the automated process, by doing a holistic review of findings to ensure that good actors were not enforced incorrectly.”

Here’s the kicker- Buy with Prime merchants can leverage these advanced capabilities for use-cases other than fraud mitigation. “As a first-time DTC seller, I had no experience in setting up an online store. The initial few months were tough as even though my site saw a good amount of traffic, the number of orders were really low”, said Charles White, owner of beverage selling company called Kombucha & You, and one of the first trial customers of this new functionality. “The high number of abandoned checkouts freaked me out and I decided to take help of Buy with Prime’s monitoring & moderation capabilities available for free on the BwP merchant console. I was pleasantly surprised when within 24 hours of me signing up, I received a report that contained a detailed analysis of each and every page of my site, broken down by sections, with every section assigned a ‘shopper trust score’ which was low in my case due to presence of shopper trust-busting attributes like poor grammar, awkward formatting, low resolution pictures etc. I was given specific recommendations and ready-to-use templates in every section to help me improve on these trust-busting attributes along with other best practice guidelines like displaying the Buy with Prime logo and having a collections page dedicated to Buy with Prime. On making changes, I submitted my site for another round of review and my ‘shopper trust score’ increased by 30 points. Confident with my site, I published the changes and I was amazed to see an immediate decrease in abandoned checkouts by 40%”

While the monitoring & moderation capabilities will help shoppers by providing a trust worthy experience, it will also help merchants maintain compliance with policies, avoiding potential account suspensions or bans. This will enable merchants to focus on growing their businesses and serving shoppers, without having to worry about violating polices. “We know that merchants and shoppers expect a trustworthy experience on Buy with Prime. Our association with Amazon brings an added layer of trust that we need to uphold at all costs”, said Peter Larsen, VP Buy with Prime. “This advanced technology will enable us to take action to remove any problematic content, such as inappropriate user-generated content, AUP non-compliant products, unauthorized use of Amazon/BwP trademarks etc. We are confident that our new capabilities will raise the bar for e-commerce safety and trust. We are excited to offer this technology to our customers and merchants and remain committed to innovate in the e-commerce space”.

For more information on the newly launched monitoring & moderation capabilities, please visit the Knowledge Centre article here: [www.buywithprime.com/monitoringmoderation](http://www.buywithprime.com/monitoringmoderation).

1. **What are we launching today? –** Today, the Santos **Fraud & Abuse Mitigation (FAM)** team is launching new monitoring & moderation capabilities to protect Buy with Prime (BwP) and Amazon against reputational, financial and compliance related risks while providing a safe and secure experience to BwP merchants and shoppers. The newly launched monitoring & moderation capabilities can be leveraged by any Santos Team to **(i)** continuously crawl and extract structured information (i.e. object/entity like product listing, image, video asset, and text string) from BwP merchants’ DTC site, and **(ii)** evaluate compliance of extracted object/entity against specific defined policies.
2. **Why are monitoring & moderation capabilities important for BwP? –** The Feb ’23 [Shopper Pulse Study](https://amazon.awsapps.com/workdocs/index.html#/document/ca7e49985c4218428cffc85df91c54400afdb45d25a29a8afe87c3576248bfe4) found that 60% of shoppers (24/40) believe the Prime badge creates a closer association between merchant’s store and Amazon in shopper’s mind. 84% of all Prime shoppers, surveyed in the [Q4 ’22 XCM Brand Tracker](https://amazon.awsapps.com/workdocs/index.html#/document/1006944013bcecf67ac2349cf9935d739d8230797f7915b80c414b38b411634c), believe Prime “is trustworthy” and 78% of all people surveyed believe that Amazon “is trustworthy” (the highest of all marketplace competitors included in the tracker). While these studies show that the Prime badge on a merchant site increases shopper’s confidence in making a purchase, the converse is also true. 8/9 shoppers, in the Jan ’23 [Brand Perception Study](https://amazon.awsapps.com/workdocs/index.html#/document/80e89ae7a9d2bf611256a239e09d7d86bffcdb7b5f98aa0cc96456062254fa40), believed that if BwP were offered for controversial items (i.e. products that represent hate speech, sexually explicit products, guns or ammo, etc.) it would reflect negatively on the Amazon/Prime brand or call into question the legitimacy of the merchant. One shopper mentioned that seeing BwP on a controversial product indicates Amazon’s mercenary intent: *“For me, it says that they’re processing those payments and it’s a way for Amazon to make money”.* Due to this close associations of BwP and Amazon in merchant and shopper mind, and important factors like ensuring compliance with laws and regulations, preventing fraud, maintaining Amazon/BwP trust and reputation, and providing a trustworthy shopping environment for shoppers, monitoring & moderating content on BwP enabled merchant sites is crucial.
3. **What are some real-life examples of problems caused due to lack of robust monitoring & moderation solutions?-** Some note-worthy examples of e-commerce companies include **(i) eBay[[1]](#footnote-0)** which faced criticism for allowing (a) price gouging during the COVID-19 pandemic with some sellers charging exorbitant prices for hand sanitizers and masks, (b) fake reviews on its platform, highlighted by an investigation by a UK consumer group which found that more than 33% of eBay sellers in UK had fake reviews on their profiles, and (c) offensive listings like Nazi memorabilia and racist merchandise on their site and (d) sale of fake designer goods for which eBay was sued by state of California in 2020 for facilitating sales of counterfeit goods and failing to take adequate steps to prevent it. Other examples include **(ii) Wish[[2]](#footnote-1),** an e-commerce platform that offers a wide range of products from 3P sellers, which faced a warning from U.S. Consumer Product Safety Commission in 2020 for sale of dangerous goods including phone chargers that posed a risk of fire and did not meet safety standards, and **(iii) Alibaba[[3]](#footnote-2)**, a Chinese e-commerce company that operates several platforms, including Taobao and AliExpress, which was added to the “Notorious Markets” list by the U.S. government in 2020 for selling counterfeit products.
4. **What is monitoring and what does it consist of? -** Monitoring is the process of extracting structured information from a website at pre-defined cadence or post a trigger activity (for e.g.: merchant adds new URL to list of URLs on which BwP widget can render) to ensure data collected is up-to-date and accurate. It consists of **(i) crawling** which is the process of automatically gathering data from a website by following links from one page to another. This is achieved through pieces of specialized software called web crawlers or spiders to navigate the site and extract data such as trademarks/logos, product details and images, general text and images on site etc., and **(ii) scraping** which involves extracting specific data from a website’s HTML code which can be used to extract data which may not be easily accessible through crawling, such as specific product attributes or pricing data. Crawling and scraping are used in conjunction to collect a wider range of data from the website.
5. **What is moderation and what does it consist of? –** Moderation is the process of evaluating data against a set of policies. It consists of **(i)** **running the extracted data through Machine Learning (ML) models** that are trained to recognize patterns and flag potential issues in data collected from monitoring activities, such as identifying potentially inappropriate content in product listings, and **(ii)** **[optional] human moderator or team of moderators** who review, based on thresholds, data flagged by ML models to determine whether the data meets established policies. Based on their findings, suitable enforcement actions are taken to mitigate the threat posed by the violation. The above steps work in conjunction with ML models helping to reduce workload for human moderators and improving the overall process efficiency/accuracy while human moderators add a layer of human intelligence rectifying any errors made by ML models. Overall, moderation plays an important role in ensuring the data collected from monitoring activities is accurate, reliable and meets established guidelines. A point to note is that monitoring & moderation capabilities can be used independently too i.e. data can be extracted and passed on without running any moderation, and content can be moderated without requiring it to be extracted through monitoring.
6. **Where do we see the most urgent need for these monitoring & moderation capabilities in BwP? –** While these monitoring & moderation capabilities shall solve several use-cases (see FAQ 14 for all use-cases), the three most urgent violation types (in priority order) that we want to mitigate are: **(i) Content violation in Santos Media Center & Catalog** that is currently unmoderated which could lead to highly offensive and reputationally damaging text/images being shown to shoppers during checkout, **(ii) Acceptable Use Policy (AUP) violation[[4]](#footnote-3)** which even though currently mitigated by EverC (a 3P compliance company) has left a lot to be desired with high number of false positives (~40%) which adds onto investigator effort, and **(iii) BwP/Amazon Trademark violations** that is currently mitigated by Incopro (a 3P brand protection company) in a time-consuming, error prone manual process, with Incopro investigators manually spot-checking every site, is not scalable as BwP expands in future.
7. **What is the end-to-end process for a URL going through FAM monitoring & moderation capabilities? –** An URL is identified (through trigger activities explained in FAQ 9) and the FAM crawler function is called. The crawler starts by sending a request to the website’s server for the initial URL and then downloads the page’s HTML content to extract all links and other information from the page. The FAM crawler function continues to follow each link it finds, downloading and processing each page it encounters. The extracted information shall include product listing, images, videos, text string, metadata and other multimedia. Once the information has been extracted from the website, a FAM function pre-processes the data (e.g.: text data to be cleaned and tokenized, image data to be resized etc.) to make it suitable for analysis. The transformed data is sent to a ML model that has been trained to classify the content based on the criteria represented in the set of guidelines. The ML model uses a variety of core capabilities like RegEx libraries, rule-based moderation, similarity algorithms, fuzzy-text matching, image recognition etc.

If there is a violation found by the ML model, it makes note of it and ranks the URL with a risk score between 0 to 99 (with 0 being least risky and 99 being most risky) based on severity and frequency of violations detected. Based on the score, the final compliance decision is one of three outcomes- *‘Compliant’, Non-Compliant’ and ‘Review Required’*. If the decision is *‘Non-Compliant’* or *‘Review Required’* a manual investigation by the FAM Risk Investigation Team (RIT) is triggered. A RIT investigator gets a notification to access a dashboard that shows the URL scanned, compliance decision, violation type and recorded evidence. The investigator verifies the violation recorded, by doing a review of the URL page(s), and marks whether site is *‘Compliant’* or *‘Non-Compliant’*. The investigator entry is used **(i)** to trigger suitable actions like enabling BwP widget or suspending BwP widget on product/domain/account depending on whether it was a true violation or not and **(ii)** as a feedback loop to improve performance of ML model. The final evaluation decision (i.e. *‘Compliant’* or *‘Non-*Compliant’) is stored by FAM Domain Service if decisions need to be persisted and potentially changed in the future.

1. **What are technical details in the working of FAM monitoring & moderation capabilities[[5]](#footnote-4)? –** At the heart of FAM monitoring & moderation capabilities is the FAM Domain Service that acts as an orchestrator by managing interactions between various components of the solution. The FAM Domain Service will manage a monitoring & moderation service responsible for **(i)** managing list of sites, **(ii)** prioritizing them based on defined metrics (e.g. traffic, number of BwP widgets, GMS etc.), **(iii)** directing the monitoring & moderation capabilities to focus on the most critical pages first **(iv)** collecting, aggregating and transforming data from site pages **(v)** understanding the business logic to be applied to the content being moderated and **(vi)** providing a centralized dashboard for investigators and storing site compliance.

The FAM Domain Service executes the above responsibilities by calling Top Level Resources (TLRs)- serverless, single purpose functions that perform specific tasks. Each violation type is created as a separate TLR (for e.g.: content violation checks on Santos Media Center & Catalog, AUP violation checks and BwP/Amazon Trademark misuse checks are created as three separate TLRs). Each TLR consists of checks needed for that particular violation type and set of guidelines against which the check is done. In some cases, depending on trigger activity (for e.g.: merchant adds a new URL), two or more checks (for e.g.: AUP violation checks and BwP/Amazon Trademark misuse check) need to be performed at the same time. For this, composite functions are created to call two or more TLRs together. Once URL is identified and monitoring & moderation capabilities need to commence, the FAM Domain Service is called which in turn calls a TLR to perform following tasks **(i)** call the FAM crawler function, **(ii)** select specific data depending on requirement (text/images for content violation check, product listing for AUP violation check, logos/banner for BwP/Amazon Trademark check) from data collected by FAM crawler function, **(iii)** pre-process selected data for analysis, **(iv)** call the ML model (which is a standalone function) and relevant parameters[[6]](#footnote-5) within the ML model to ensure that data meets specific guidelines (the guidelines may vary for each TLR, for example BwP AUP for content checks on Santos Media Center & Catalog, APay AUP for AUP violation checks, and BwP Brand Guidelines for BwP/Amazon Trademark misuse check), and **(v)** trigger manual investigation based on URL risk score and power centralized dashboard for investigators.

1. **What activities will trigger FAM monitoring & moderation capabilities? –** All URLs on which a BwP widget can render as well shall be monitored & moderated at a regular pre-defined cadence (daily/weekly/monthly). There is also flexibility to customize different cadences for different violation types, for e.g.: AUP violation checks can be performed daily but BwP/Amazon Trademark misuse checks can be performed weekly. Additionally, arrival of any holiday/ sales event (e.g.: Prime Day, Black Friday, Cyber Monday) that has historically triggered huge sale numbers shall result in more frequent monitoring & moderation of URLs so that any violation flagged can be quickly mitigated. Apart from pre-defined cadence scans, there are seven activities that shall trigger ad-hoc checks: **(i)** merchant adds new URL to list of URLs on which BwP widget can render, **(ii)** first BwP transaction on merchant site, **(iii)** rapid increase in traffic or sales on merchant site, **(iv)** Seller Risk Score (SRS) of BwP merchant crosses defined threshold, **(v)** merchant flagged by other FAM solutions like RRD/ODR, **(vi)** merchant appeals to get account re-instated and **(vii)** escalations/ shopper feedback about violations on a URL.
2. **What factors will determine priority order of URLs for monitoring & moderation? –**To calculate the GV-weighted coverage of the monitoring & moderation capabilities, and allow for more efficient use of resources, URLs will be prioritized using the following factors: **(i) site traffic** since violation on a high traffic site will be seen by more shoppers than on low/to no traffic site **(ii) number of BwP widgets on site** as chances of a violation being associated with BwP widget increase with more widgets on site, **(iii) Google/Bing search rank** since violations on URLs that consistently rank higher in search results for relevant keywords are easily findable and accessible to shoppers, and **(iv) merchant volume (units sold)** since we want to ensure that our highest unit drivers do not have a violation that may lead to reputational concerns for Amazon/BwP
3. **What are the milestones for this project[[7]](#footnote-6)? –** FAM team will launch monitoring & moderating capabilities as a series of functionalities that will be released in stages, culminating in an end-state product. These functionalities will be combined to create a comprehensive monitoring & moderation solution, providing users with a seamless and effective tool for managing content and ensuring compliance. The phased rollout will allow for gradual integration of each functionality, ensuring smooth and effective adoption of the final product.

The high-level milestones for a phased launch of monitoring capabilities are: **(i) Milestone 1:** Support keyword-based monitoring to identify specific words/phrases, **(ii) Milestone 2:** Support image recognition to detect and flag high-risk images, and **(iii) Milestone 3:** Extract advanced features from website like video, audio, metadata, website performance etc., and **(iv) Milestone 4:** Initiate event and alert based monitoring by triggering monitoring after specific events/alerts occur (for example: unusual spike in traffic)

The high-level milestones for a phased launch of moderation capabilities are: **(i) Milestone 1:** Create a RegEx Based Library to detect specific inappropriate keywords in given content, **(ii) Milestone 2:** Deploy a rule-based system for text moderation based on pre-defined rules, **(iii) Milestone 3:** Support image moderation by creating rules/heuristics to recognize specific patterns or features in images, and **(iv) Milestone 4:** Develop a ML model to support text and then image moderation. Incrementally add features to the ML model like sentiment analysis,

1. **Apart from BwP enabled merchant sites, which other domains will we monitor & moderate? -** While our first priority is to monitor & moderate BwP enabled merchant URLs, it is also important to track 3P domains, social media sites, Appstore pages, marketplace sites etc. in order to **(i)** catch unauthorized use of Amazon/BwP brands names and trademarks, and **(ii)** check for BwP related mentions on social media, using it as a mechanism to inform product strategy. While we have not included scanning the Internet in FAM monitoring & moderation capabilities, we will continue to leverage external solutions to solve for **(i)** and **(ii)** as we do today. For **(i)**, we leverage Incopro to scan 3P sites based on keywords and BwP logos every week[[8]](#footnote-7), and for **(ii)** FAM team recently created a [social listening handle for BwP](https://external.sprinklr.com/research/insights/listening/dashboard/5b5d8d26e4b0f6cf9abe81f1/tab/1?id=1A66641C631BBD05F281D996F5E08D5F5AC1632E20282D9880A925FF1363A25F) with help from Selling Partner Communities Team that listens across all major social channels and forums for specific tags, and gets insights with sentiment analysis.
2. **How can Santos Product Teams leverage FAM monitoring & moderation capabilities? –** The FAM Domain Service acts as a cross-functional platform providing monitoring & moderation capabilities that can be integrated into different Santos teams’ workflows. Santos teams can onboard onto the FAM Domain Service, and create specific TLRs for their use-case (consisting of relevant checks and specific guidelines against which checks are run). The TLR calls specific parameters of ML model as per outcome needed by domain teams. Domain Teams can use specific capabilities too (like only monitoring or only moderation) as per their use-case. Inputs into FAM Domain Service will be the details to be evaluated against the relevant policy, and primary output is a response of *'Compliant,' 'NotCompliant,'* or, optionally based on configuration, *'Review Required.'* FAM Domain Service will return which requirement(s) led to a *‘NotCompliant’* or *‘Review Required’* outcome and shall either just pass this decision to Santos team, or Santos team may leverage FAM Risk Investigations Team (RIT) to perform additional manual review.
3. **Apart from the priorities called out in FAQ 6, what are other use-cases in which Santos product teams can leverage monitoring & moderation capabilities?** *(not exhaustive)* –

Santos product teams can leverage monitoring & moderation capabilities: **(i) to mitigate unauthorized or fake[[9]](#footnote-8) Reviews from Amazon (RFA) widget or reviews in general** by scanning DTC sites for RFA widgets/shopper reviews and detecting content violations as well as fake/malicious reviews, **(ii) to moderate listings[[10]](#footnote-9) in Santos Catalog for Restricted Product Policy Compliance** by checking the Santos Catalog against relevant policy guidelines or running a gap analysis between Amazon Catalog and Santos Catalog and moderating the differences, and **(iii) to moderate merchant-submitted labels as part of BwP Shops Subdomain** by doing keyword analysis to check for infringement, profanity or potential security issues.

Apart from fraud mitigation use-cases, there are opportunities to better BwP experience for merchants/shoppers by leveraging monitoring & moderating capabilities: **(i) to suggest improvements to merchant site[[11]](#footnote-10)** by scanning their sites and providing a detailed report that ranks and suggests improvements in areas such as image formatting, grammar, picture resolution etc., **(ii) to provide merchants feedback of their services** by combining trend analysis, seller reputation, shopper feedback, product quality management and price monitoring into a dashboard view to help merchants improve their performance, **(iii) to provide merchants sentiment analysis of customer reviews** to identify areas of improvement and help merchants optimize product listings, and **(iv) to ensure that BwP sites are easily navigable by shoppers[[12]](#footnote-11)** by scanning to check whether merchants are following best practices like having a FAQ page, or a BwP collections page or calling out return instructions clearly etc.

1. **Does FAM team have any existing monitoring & moderation capabilities as of today? –** Yes. The FAM Team currently has three existing monitoring & moderating capabilities (either by leveraging third parties or through a manual process) which are: **(i)** AUP violations check conducted by EverC (a 3P compliance company) which scans products & product listings on BwP enabled sites against APay AUP policy at a monthly cadence. The FAM team is working with EverC to set up a daily scan so that BwP enabled sites are monitored at a more frequent cadence and any violations are mitigated as soon as possible. **(ii)** BwP/Amazon Trademark misuse check conducted by Incopro (3P brand protection company) at a weekly cadence. Incopro investigators manually spot-check BwP sites to scan for trademark/logo misuse. Additionally, Incopro also monitors 3P domains, social media sites, marketplaces and Appstores for keywords like ‘Buy’ and ‘Prime’, BwP badges and Prime smile logo, and flags unauthorized use of BwP/Prime materials on the internet, and **(iii)** random audits done by RIT investigators on BwP enabled sites to check for any violations on the site.

1. **What are some of the existing monitoring & moderation capabilities in Amazon as of today? –** Based on our deep dive we found some teams in Amazon that have existing monitoring & moderation capabilities like: **(i) Classification & Policy Platform (CPP)[[13]](#footnote-12)** which provides self-service classification of products in the catalog and management of policies based on classifications by business users, **(ii) Selection Monitoring Team[[14]](#footnote-13)** which provides data about external selection to Amazon to help improve customer experience by adding to catalog, keeping prices sharp and improving availability, **(iii) Competitor Monitoring Team[[15]](#footnote-14)** whose primary objective is to provide accurate and timely information about competitor’s price and other dimensions such as availability, promotions, ship price and rebate which are relevant to customer’s purchasing decisions, **(iv) Amazon Community Shopping Team** whose ML model and blocklists were leveraged by Santos Reviews & Ratings team for review moderation and **(v) Amazon Rekognition[[16]](#footnote-15)** which is a ML based AWS service with great capability to detect inappropriate, unwanted, or offensive image content while also covering more general categories. It is the new solution Amazon Community Shopping team plans to adopt in 2023.
2. **Why can’t we keep leveraging 3P solutions instead of building in-house monitoring & moderation capabilities? –** There are two main reasons to not keep leveraging 3P solutions: **(i) Increasing cost as the BwP program scales:** The cost of EverC to monitor ~12000 merchants[[17]](#footnote-16) (assuming each merchant has 1.5 URLs on average) is ~750k $ annually. Similarly, Incopro charges ~850k $ to scan 5000 merchant sites[[18]](#footnote-17) every month. Apart from the fact that these costs will almost scale linearly with number of merchants/URLs, the varied number of monitoring & moderation use-cases that we have to solve in the next few years, will require different contracts with different 3P solutions[[19]](#footnote-18) leading to a high operations load. **(ii) Lack of control over mechanism:** We currently do not have any control on the monitoring & moderation processes of EverC and Incopro which leads to missed violations, incorrect enforcements and false positives. To add one, there is also dependency and data sharing threats associated with 3P solutions.

**Recommendation-** The FAM Team’s recommendation is to build our own in-house monitoring & moderation capabilities and reuse parts of existing Amazon services (as detailed in FAQ 16) as applicable.

1. **What are the next steps? –** The FAM Team will be building a proof-of-concept of a specific use-case (TBD) leveraging the monitoring & moderation solution and is tracking it as a team level goal this year (ETA: Q3 2023)

1. Source: [Reuters](https://www.reuters.com/article/uk-ebay-holocaust-idUKBRE9A10B920131102) [↑](#footnote-ref-0)
2. Source: [New York Times](https://www.nytimes.com/2022/07/07/business/media/wish-online-dollar-store.html) and [Reuters](https://www.reuters.com/technology/french-regulators-lift-ban-online-marketplace-wish-2023-03-14/) [↑](#footnote-ref-1)
3. Source: [Reuters](https://www.reuters.com/business/china-leads-world-counterfeit-pirated-products-us-report-2023-01-31/) [↑](#footnote-ref-2)
4. AUP violation check also scans for violations other than those on products or PDP pages on the merchant site (e.g.: violation on ‘Contact Us’ page) [↑](#footnote-ref-3)
5. This is an overview of possible technical implementation detail which will vary once we land on a high-level design [↑](#footnote-ref-4)
6. Parameters shall include specific algorithms like fuzzy-text matching or similarity algorithms [↑](#footnote-ref-5)
7. These milestones are at a high level and there will be more granular milestones than the ones described here [↑](#footnote-ref-6)
8. Incopro’s keyword and logo search has flagged 25,924 sites till date. Out of these 16 sites were flagged to FAM team and has been forwarded to Amazon IP Legal [↑](#footnote-ref-7)
9. Bad actors might either (a) scrape Amazon reviews and display them on DTC in unauthorized fashion or (b) create a widget that looks and feels like RFA and stuff it with fake reviews. [↑](#footnote-ref-8)
10. Amazon.com product listing controls which are enforced when merchant creates a listing in Amazon catalog (currently required to fulfill product through MCF/BwP). This mitigation can be circumvented, however, as there is no requirement that Amazon Catalog and Santos Catalog have same content/images [↑](#footnote-ref-9)
11. All shoppers (40/40) in the BwP Brand Perception Study mentioned that they are more likely to abandon purchase from a site that has trust busting attributes on the site like low-resolution photography, awkward formatting and poor grammar [↑](#footnote-ref-10)
12. We are currently leveraging Incopro to provide us with a report on how many merchants are following the best practice guidelines [↑](#footnote-ref-11)
13. Source: [Classification & Policy Platform (CPP)](https://w.amazon.com/bin/view/ASCS/CPP/) [↑](#footnote-ref-12)
14. Source: [Selection Monitoring Team](https://w.amazon.com/bin/view/SelectionMonitoring/) [↑](#footnote-ref-13)
15. Source: [Competitor Monitoring Team](https://w.amazon.com/bin/view/CMT/) [↑](#footnote-ref-14)
16. Source: [Amazon Rekognition](https://docs.aws.amazon.com/managedservices/latest/userguide/rekognition.html) [↑](#footnote-ref-15)
17. BwP is forecasted to have ~12000 total merchants by the end of 2023 [↑](#footnote-ref-16)
18. This is maximum pricing provided by Incopro. As of present contract, Incopro is scanning 1000 merchants per month for ~320k $ annually [↑](#footnote-ref-17)
19. Incopro only solves for BwP Trademark misuse while Incopro only solves for AUP violations [↑](#footnote-ref-18)