ORGANIZED RETAIL CRIME TASK FORCE



2024 WASHINGTON STATE ATTORNEY GENERAL'S OFFICE



Survey of Online Marketplaces

Acknowledgement

This report is only possible through the voluntary participation of many online marketplaces. The Attorney General's Office appreciates their participation in this project and their willingness to share information about their processes.

The Attorney General's Office (AGO) convened the Organized Retail Crime Task Force (ORC Task Force) to help improve collaboration and coordination to address organized retail crime in the state. The Task Force brings together local, state, and federal law enforcement representatives, as well as retail partners and online marketplaces, to address multi-jurisdictional crimes perpetrated by organized crime rings. There are currently 325 representatives on the ORC Task Force. To date, the ORC Task Force has convened five meetings. One goal of the ORC Task Force includes establishing and circulating best practices for addressing organized retail crime, which endangers consumers and workers, harms businesses, and damages the economy. The Task Force identified the reselling of stolen merchandise on online marketplaces as a priority. Improving coordination and collaboration between online marketplaces, law enforcement and brick-and-mortar retailers is one way to help address this problem. Online marketplaces are one means, though not the sole means, by which organized crime rings sell stolen goods.

The purpose of this report is to provide the public, law enforcement, and businesses impacted by organized retail crime with additional information and insights into the efforts online marketplaces are making to combat organized retail crime. Additionally, this report provides the marketplaces with information about the actions other marketplaces are taking so that they may adopt best practices.

Organized Retail Crime: Online Marketplaces Report Efforts to Combat Trafficking of Stolen Property, But More Can Be Done to Implement Promising Practices

The AGO met with dozens of retailers, union representatives, online marketplaces, and law enforcement agencies both in Washington state and beyond. Based on that outreach, in November 2022, the AGO sent a letter to online marketplaces sharing preliminary recommendations for combating organized retail crime on their platforms and urging their adoption (see Appendix 1).

In their responses, most of the online marketplaces provided an overview of actions they take to address content that violates their policies or amounts to fraud or illegal activity, not all of which is organized retail crime.

The AGO's preliminary guidance to online marketplaces highlighted the need for specialized, dedicated processes addressing organized retail crime and trafficking on the online platforms. The AGO recommended measures including:

- Establishing a specialized ORC team dedicated solely to interfacing with victims and law enforcement to investigate trafficking on the marketplace.
- Establishing mechanisms for sharing information and data about suspect sellers and sales history with victims and law enforcement on an expedited basis.
- Identifying the types of items regularly sold on the marketplace that are particularly susceptible to trafficking.
- Providing retailers with periodic reports about the types of items identified as susceptible to trafficking on the platform, the geographic areas in which such items are commonly sold, and other trends.

Methodology

Between November 2022 and March 2023, the AGO surveyed nine online marketplaces to further understand how they combat trafficking of stolen property on their platforms. Seven online marketplaces voluntarily provided information to the AGO. The findings reflect the online marketplaces' practices at that time.

eBay and OfferUp responded directly to the AGO's survey seeking information on whether the marketplaces have implemented the preliminary guidance. Upon follow-up with AGO staff, OfferUp provided additional information on how they combat ORC on their platform, see Appendix 3. The remaining marketplaces sent letters.

Summary of Responses

Finding 1

All the marketplaces that responded reported having mechanisms in place to respond to law enforcement; however, only Amazon, eBay, and OfferUp reported having a specialized ORC team.¹

| Online Marketplace | Mechanism for Law Enforcement Requests | Specialized ORC Team Interfacing with Law Enforcement |
|--------------------|---|--|
| Amazon | \checkmark | \checkmark |
| Craigslist | No response | No response |
| eBay | \checkmark | \checkmark |
| Etsy | \checkmark | Information not provided |
| Mercari | \checkmark | Information not provided |
| Meta | \checkmark | Information not provided |
| Nextdoor | \checkmark | Information not provided |
| OfferUp | \checkmark | \checkmark |
| Overstock | No response | No response |

While all marketplaces that provided information to the AGO indicated that they respond to law enforcement requests, few stated that they have developed specialized ORC teams dedicated to interfacing with victims and law enforcement solely to investigate trafficking of stolen property through their marketplace. eBay was the only marketplace that provided information about its team's typical response time to trafficking inquiries. It is not clear whether or not other marketplaces respond promptly. Moreover, eBay was the only marketplace that explicitly addressed responding to victim inquiries.

Online marketplaces offer different avenues for law enforcement to contact them: three have dedicated email addresses for law enforcement and five have online submittal tools for requests for records (with one marketplace offering both). Appendix 2 shows the contact information and online portals that marketplaces have made available.

In addition, Amazon and OfferUp provide online guidance for law enforcement, which can be viewed by clicking on the links in the endnote.²

Spotlight: Mechanisms for Engaging Law Enforcement

eBay

eBay responded that it has a specialized organized retail crime team to engage victims and law enforcement as part of trafficking investigations. With four dedicated staff on the team, along with mechanisms for law enforcement and victims to reach the team via email, eBay responds to inquiries within 72 hours on average, and its standard service occurs within 10 days. eBay's Security Center webpage provides information for law enforcement to contact eBay with questions on how to request records and use its law enforcement eRequest tool.³ It also directs customers to contact local police to obtain a crime reference number if they have been defrauded by a seller or have reason to believe that they have discovered stolen goods. The investigating officer may then contact eBay, and eBay can provide information to law enforcement to help with the investigation.

OfferUp

OfferUp serves as another example of a marketplace tackling organized retail crime through its partnerships with law enforcement, retailers, and other online marketplaces. OfferUp has a four-person Investigations team that prevents and responds to criminal and fraudulent activity. OfferUp assisted with over 1,100 organized retail crime cases in 2023, as of 3/28/2023, resulting in multi-million dollar recoveries and criminal prosecution.

Amazon

Amazon has a specialized ORC Engagement Team (known as ORCET) made up of individuals with law enforcement backgrounds who are dedicated to interfacing with retailers, law enforcement, and others to combat ORC.

Opportunities for New Best Practices

- Streamline communication with law enforcement and victims of ORC by establishing and making available criteria for when and how a marketplace will investigate ORC.
- Create mechanisms to provide timely responses to victims.

Finding 2

Most online marketplaces reported multiple methods to detect prohibited content, including automated systems and human review. Some online marketplaces also provide guidance to users on detecting and avoiding fraud and scams.

All of the marketplaces addressed ways in which they identify problematic listings, and specifically mentioned automated processes they utilize in addition to human review. Marketplaces like eBay, OfferUp, Meta, and Nextdoor also shared additional resources they have developed to help users identify problematic postings.

| Online Marketplace | Automated review system | Guidance to Users on Avoiding Frauds and Scams |
|--------------------|-------------------------|--|
| Amazon | \checkmark | \checkmark |
| Craigslist | No response | No response |
| eBay | \checkmark | \checkmark |
| Etsy | \checkmark | Information not provided |
| Mercari | \checkmark | Information not provided |
| Meta | \checkmark | \checkmark |
| Nextdoor | \checkmark | \checkmark |
| OfferUp | \checkmark | \checkmark |
| Overstock | No response | No response |

2024 Organized Retail Crime Report

Spotlight: Mechanisms to Identify Problematic Listings

eBay

In addition to human review, eBay uses automated filters to detect prohibited content. eBay also provides a variety of information and guidance to their users on how to avoid scams and how to buy and sell on the site safely.⁴

Mercari

Mercari uses keyword detection via "auto-reports" that create alerts based on certain words used in a product listing, which can then be reviewed by Mercari's Trust and Safety Team to determine any necessary action. Other methods include artificial intelligence detection models for identifying items undetected by keyword detection, proactive monitoring by Mercari agents who manually review new listings and conduct ad-hoc searches for violating items, and reviewing listings reported by Mercari community members.

Meta

Meta's automated system proactively checks each listing to detect stolen goods. Meta relies on human review teams to build and train its systems and occasionally conduct manual review of listings. A majority of the listings that violate Meta's policies are rejected through this process before going live, but listings can also be re-reviewed in response to user feedback. Users are directed to report suspicious listings to Meta and to contact their local law enforcement to file a police report if stolen items are listed on Facebook Marketplace. When Meta is notified of listings of potentially stolen items, they investigate and remove listings, buyers, or sellers when appropriate.

To help customers avoid fraud, Meta provides shoppers with educational modules and tips to avoid scams and shop responsibly on their platform, including researching products and sellers before completing a transaction and using secure payment methods.

Nextdoor

Nextdoor reported that they use tools to automatically detect harmful content as well as trained specialists who review content and accounts that have been flagged—by both the automated system and users—and take appropriate action.

To help customers avoid fraud, Nextdoor cautions users about expensive items listed at prices well below market value, particularly vehicles and electronics.⁵ The marketplace also notes that fraudulent sellers may request payment in the form of gift cards and then fail to deliver on the sale.

OfferUp

OfferUp has developed other strategies to meet their users' unique needs. OfferUp's marketplace is primarily a local face-to-face experience, which necessitates focusing on users' physical safety. OfferUp has worked with law enforcement to develop a list of "safe meetup spots" for their users.

Opportunities for New Best Practices

- Utilizing both user reporting of suspect listings and/or sellers and automated review systems is good practice because it can help bolster efforts to identify problematic listings, rather than systems that rely on only one method of detection. Marketplaces can better leverage user reporting by making information on how to report suspicious listings more accessible and prominent on the marketplace's platform.
- Providing users with resources and guidance for identifying scams and problematic listings is good practice, but this information needs to be more prominently displayed and available to users to review before completing purchases. For example, marketplaces can proactively and prominently warn buyers to be wary about items offered at prices substantially below the manufacturer's suggested retail price. These resources should be translated and made available in multiple languages.

2024 Organized Retail Crime Report

Finding 3

Amazon, Mercari and OfferUp have specialized responses to products that are susceptible to trafficking.

A few online marketplaces have developed special policies and practices for items that are of greater risk of being stolen and resold on online marketplaces, such as mobile phones, power tools, over-the-counter pharmaceuticals, and items that are in short supply (e.g., baby food during the 2022 shortage).

| Online Marketplace | Response to High-Risk Products |
|--------------------|---------------------------------------|
| Amazon | \checkmark |
| Craigslist | No response |
| еВау | \checkmark |
| Etsy | Does not sell these types of products |
| Mercari | \checkmark |
| Meta | Information not provided |
| Nextdoor | Information not provided |
| OfferUp | \checkmark |
| Overstock | No response |

Spotlight: Identifying Items Susceptible to Trafficking

eBay

eBay has developed an internal list of types of products regularly sold through their marketplace that are particularly susceptible to trafficking, such as consumer electronics. For these items, eBay requires additional information from sellers before the item can be listed, including financial or bank account information and authentic or unedited photographs of the item for sale. This information is reviewed, and if found to be false, eBay will stop or suspend the sale.

Amazon

Amazon also requires sellers to request approval for some categories of products. Sellers can find the requirements for different product categories online.⁶ For example, products listed in the jewelry category must be authentic (not counterfeit or replica) and must meet Amazon's Jewelry Quality Assurance Standards.

Mercari

Mercari also has strategies around high-risk products. Mercari utilizes several detection methods and proprietary systems to identify and flag potentially problematic listings, including the use of brand or item-specific rules, often created through consultation with brand owners or industry contacts. Mercari has established rules based on product inconsistencies, pricing variation, inconsistent trademarks, names or logos, and other industry guidance. Mercari contracts with a third-party to review listings using their proprietary detection methodology, and requires a separate authenticity review by an independent third-party service provider for certain items within a specific luxury category. Items flagged by the third-party service as non-authentic cannot be listed.

Opportunities for New Best Practices

- Some marketplaces identify the types of items regularly sold through their marketplace that are particularly susceptible to trafficking. More marketplaces should consider adopting this approach.
- Some marketplaces utilize third-party contractors to identify problematic postings. More marketplaces should consider this approach to tackling organized retail crime.
- Online marketplaces should also work to identify any purportedly new items being offered at prices substantially below the manufacturer's suggested retail price.

2024 Organized Retail Crime Report

- Given that only a few marketplaces highlighted their specialized approach to high-risk products, there are opportunities for marketplaces to make requirements for sellers more robust. For example, if it is not already a requirement, sellers should be required to post authentic and unedited photographs for any listings of new and unused packaged goods and for any used or unpackaged consumer electronics, including the item's stock keeping unit number, bar code, or serial number.
- For high-risk products and purportedly new products being offered at prices substantially below the manufacturer's suggested retail price, sellers should be required to provide additional information, including documentation firmly establishing the identity of the seller, verification of the seller's physical address, and financial or bank account information for the seller's account.

Finding 4

All responding marketplaces have rules or terms that feature a list of prohibited items and services.

In addition to stolen goods, online marketplaces prohibit a variety of other items from being sold on their platforms.

| Online Marketplace | List of prohibited items |
|--------------------|--------------------------|
| Amazon | \checkmark |
| Craigslist | No response |
| еВау | \checkmark |
| Etsy | \checkmark |
| Mercari | \checkmark |
| Meta | \checkmark |
| Nextdoor | \checkmark |
| OfferUp | \checkmark |
| Overstock | No response |

Spotlight: Prohibited Items and Services

Etsy

Etsy's "House Rules" require items advertised as handmade to be made or designed by the seller, and prohibit the reselling of most items, with the exception of craft supplies, which Etsy views as a low-risk category when it comes to organized retail crime. In Etsy's opinion, they do not allow categories of goods which are most susceptible to organized retail theft, "scarce or valuable commodity-type items," such as mobile phones, over-the-counter pharmaceuticals and infant formula. To detect prohibited items, Etsy reported that they review tens of thousands of listings each week and remove non-handmade items.

Mercari

Mercari's prohibited items list includes anything illegal, unsafe, or potentially harmful, such as air bags, counterfeit goods, and infant formula.

Nextdoor

Nextdoor prohibits items sold by resellers and commercial consignment and estate sellers in its "For Sale & Free" sections, where neighbors post items they are selling or giving away.

Finding 5

Under the INFORM Consumers Act, all the online marketplaces have privacy policies for users which govern how information is shared with law enforcement and other entities.⁷

The privacy policies of all online marketplaces explain the data that is collected from users and sellers, and how data may be shared as part of law enforcement investigations in cases of illegal activity. In addition to highlighting privacy policies, Amazon, Mercari, Meta, and Nextdoor also highlighted their efforts at seller vetting.

| Online Marketplace | Seller Vetting |
|--------------------|--------------------------|
| Amazon | \checkmark |
| Craigslist | No response |
| eBay | \checkmark |
| Etsy | Information not provided |
| Mercari | \checkmark |
| Meta | \checkmark |
| Nextdoor | \checkmark |
| OfferUp | \checkmark |
| Overstock | No response |

Spotlight: Mechanisms to Verify Seller Identity

Amazon

Amazon uses a combination of technology and human reviews for its seller vetting process. Prospective sellers are required to provide a government-issued photo ID, location, taxpayer information, bank account, credit card, and more. Amazon's proprietary systems analyze hundreds of unique data points to verify the information and detect potential risk. Additionally, all prospective sellers who want to sell in Amazon's U.S. store are required to have one-on-one conversations with one of Amazon's team members and provide documentation to verify their identity.

eBay

eBay verifies the identity details for those who register for seller accounts on the site. Sellers are required to provide their full name, address, date of birth, and social security number. If selling as a registered business, the seller must also provide information about the business.

Meta

Meta has a verification system for high-volume third-party sellers. Sellers who have sold more than \$5,000 across at least 200 transactions in any 12-month period over the past 24 months are required to provide information about their business, including business name and address, tax ID, and customer support contact details. Meta verifies this information and provides it to buyers.

Nextdoor

All Nextdoor users, including those who sell in the "For Sale & Free" marketplace, go through verification. Nextdoor verifies individuals and businesses using signals, such as device location and third-party data. If Nextdoor cannot verify an individual or business with a phone call or text, the marketplace may mail a postcard with a code to the individual's address.

Opportunities for New Best Practices

- Online marketplaces should establish mechanisms for sharing data about suspect sellers and their
 sales histories with victims and law enforcement on an expedited basis, without disclosing personal
 information about the seller that is protected by law. The AGO's survey queried online marketplaces about
 implementing this recommendation, but did not receive responsive answers.
- Online marketplaces should consider creating and sharing criteria with investigators regarding the timing and extent to which they can provide information about suspect sellers on an expedited basis and without requiring formal legal requests.

Finding 6

eBay shares periodic reports about trafficking on their site, while Etsy and Amazon publish reports about safety and brand protection.

While eBay specifically provides retail partners with reports about trafficking on their site, Amazon and Etsy shared published reports that offer information about how the sites tackle counterfeit products on their marketplaces, among other concerns.

| Online Marketplace | Provide Reports About Site Safety |
|--------------------|-----------------------------------|
| Amazon | \checkmark |
| Craigslist | No response |
| еВау | \checkmark |
| Etsy | \checkmark |
| Mercari | Information not provided |
| Meta | Information not provided |
| Nextdoor | Information not provided |
| OfferUp | Does not publish public reports |
| Overstock | No response |

Spotlight: Sharing Safety Information

eBay

eBay provides periodic reports about the items found to be susceptible to trafficking on their site, including geographic areas where such items are sold, so retailers can make informed decisions about adjusting their sales practices to protect their inventory. eBay also provides reports upon request from their PROACT partners. The PROACT program is a two-way reporting system in which retailers can warn eBay that they have had a significant theft and inform them of the items stolen, and then eBay can watch for matching items to appear for sale on its site. eBay reports that the PROACT team has enlisted over 60 retailers to join the PROACT program and provide the team with leads on potentially harmful sellers.⁸

Etsy

Etsy's "Trust & Safety" efforts aim to address policy violations, such as listing new commercial items in Etsy's handmade category. In 2021, Etsy received 17 million flags of potentially non-compliant listings, 87% of which were generated by its internal automated systems, while 13% were generated by community users. Around 16% (or 2.7 million) of these flags resulted in actions by Etsy's agents or automated systems. Etsy removed 346,408 listings for counterfeiting violations and closed 27,979 shops for repeat violations of intellectual property and counterfeiting rules. Etsy also produced records in response to 212 of 237 legal requests, which requested information relating to one or more members, transactions, listings, and other content on the marketplace. Etsy disclosed such requests to 806 affected members.

Amazon

Amazon's Brand Protection Report highlights the successes of its vetting process, through which Amazon has stopped over 2.5 million attempts to create new selling accounts before they were able to publish any products for sale.⁹

Opportunities for New Best Practices

• Similar to the work eBay does as part of their PROACT program, online marketplaces should partner with retailers and provide them with periodic reports about the types of items identified as susceptible to trafficking on their marketplaces, the geographic areas in which such items are commonly sold, and any other trends that would enable retailers to adjust their sales practices accordingly and protect their inventory.

Conclusions and Next Steps

This report serves as a resource for law enforcement, business, workers, and other Task Force members working to combat organized retail crime, who may have reason to work with online marketplaces.

Online marketplaces are working to combat organized retail crime, but more can be done. Each online marketplace should strongly consider adopting the best practices outlined in this report, especially the practices that are working for other marketplaces.

Endnotes

1 The survey defined a specialized ORC team as one with members specifically dedicated to interfacing with victims and law enforcement to investigate trafficking of stolen property through their respective marketplaces.

2 <u>https://d1.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf; https://help.offerup.com/hc/en-us/articles/360032336811-Law-Enforcementresources.</u>

3 The eBay Law Enforcement eRequest System enables law enforcement officers seeking records for investigations to quickly and securely request this data: <u>https://le.corp.ebay.com/leportal_communitieslogin</u>.

- 4 <u>https://pages.ebay.com/securitycenter/index.html</u>.
- 5 <u>https://help.nextdoor.com/s/article/Known-Scam-Bargain-vehicles-in-For-Sale-and-Free?language=en_US.</u>
- 6 <u>https://sellercentral.amazon.com/help/hub/reference/external/G200333160</u>.

7 The INFORM Consumers Act became effective on June 27, 2023. Under the new law, online marketplaces must collect, verify, and disclose certain information about "high-volume third party sellers."

6 <u>https://pages.ebay.com/securitycenter/law_enforcement.html#law_enforcement_content.</u>

7 <u>https://brandservices.amazon.com/progressreport.</u>

Appendix 1: Letter to Online Marketplaces



Bob Ferguson ATTORNEY GENERAL OF WASHINGTON

Consumer Protection Division 800 Fifth Avenue • Suite 2000• MS TB 14 • Seattle WA 98104-3188 (206) 464-7744

November 2, 2022

RE: Combating Organized Retail Crime

To Whom It May Concern,

Earlier this year, I convened the Washington State Organized Retail Crime Task Force. The growth of organized retail crime is causing billions in economic harm to Washington businesses, and frequently includes violence or threats of violence against employees of those businesses. The Task Force is working to combat organized retail crime, improve coordination among law enforcement and interested parties, and identify areas of potential collaboration with stakeholders including online marketplaces.

I appreciate the online marketplaces that are participating in the Task Force. Organized retail crime involves theft of retail products for resale, and one of the Task Force's primary goals is to identify ways to hinder criminal actors' efforts to resell stolen goods through online marketplaces. You are uniquely positioned to assist in this regard.

Since the Task Force's initial public meeting on July 7, 2022, the Attorney General's Office met with dozens of retailers, union representatives, online marketplaces, and law enforcement both in Washington State and beyond. Based on that outreach, the Attorney General's Office developed the following primary recommendations for online marketplaces. We believe these are commonsense steps to combat organized retail crime. We understand through our outreach that some marketplaces have already adopted several of these reforms, earning praise from retailers. We commend those efforts and urge universal adoption of each of these basic and necessary measures:

- 1. Establish a specialized organized retail crime team dedicated solely to interfacing with victims and law enforcement to investigate trafficking of stolen property through your marketplace. The team should be sufficiently robust to provide requested information and assistance in an expedited manner, and should include a mechanism for victims and law enforcement to contact your team members directly and receive a prompt reply.
- 2. Establish and make available the team's criteria for assisting victims and law enforcement with such trafficking investigations. These criteria should include guidance regarding what information you require for identifying a suspect seller, suspected stolen property, the victim's basis to believe that stolen property is being or has been trafficked

ATTORNEY GENERAL OF WASHINGTON

November 2, 2022 Page 2

through your marketplace, and any other information necessary to trigger the assistance of your team.

- 3. Establish mechanisms by which information and data about the suspect seller and their sales history may be shared with victims and law enforcement on an expedited basis, without disclosing personal information about the seller that is protected by law.
- 4. Identify the types of items regularly sold through your marketplace that are particularly susceptible to trafficking. Examples of items particularly susceptible to trafficking may include, for example, mobile phones, power tools, over-the-counter pharmaceuticals, and items that are in short supply, e.g., baby food during the 2022 shortage. The Task Force is available to collaborate on the identification of additional such items.
- 5. Identify purportedly new items being offered at prices substantially below the manufacturer's suggested retail price (MSRP).
- 6. For the items referenced in recommendations #4 and #5 above, require sellers of such items to provide additional information prior to making their offers viewable to the public. The additional information should include documentation firmly establishing the identity of the seller, verification of the seller's physical address, financial or bank account information for the seller's account, authentic and unedited photographs of the item(s) for sale, and a statement or documentation from the seller about the origin of the item(s). Because criminal actors frequently open new seller accounts with online marketplaces to traffic stolen property, and because once opened such seller accounts may persist in trafficking stolen property even in the face of investigations, these criteria should be applied for all new accounts and for accounts that have previously been the focus of your team's trafficking investigations, law enforcement inquiries, or complaints from victims and retailers.
- 7. Modify your sales terms to require that, as part of any marketplace sale of a new and unused packaged good, the seller must post authentic and unedited photographs of the item for sale, including depictions of the item's stock keeping unit (SKU) number and bar code.
- 8. Modify your sales terms to require that, as part of any marketplace sale of used or unpackaged consumer electronics, the seller must post authentic and unedited photographs of the item for sale, including depictions of the item's identifying serial number where one exists.
- 9. Provide retailers with periodic reports about the types of items identified as susceptible to trafficking through your platform, the geographic areas in which such items are commonly sold, and any other trends that would enable retailers to adjust their sales practices accordingly and protect their inventory.

ATTORNEY GENERAL OF WASHINGTON

November 2, 2022 Page 3

The next public meeting of the Task Force is on November 30, 2022. I hope you will attend. Prior to November 30, please let the Attorney General's Office know whether you will implement these recommendations. If you cannot implement them prior to November 30, please let us know your anticipated timeline for implementation. If you are declining to implement these recommendations, please let us know prior to November 30 of your reasons.

Finally, we will also be sending surveys to assess your current practices and capabilities in this regard. Please let us know to whom we should direct the survey.

Should you have any questions relating to this letter, please contact Joe Kanada or Ben Carr at joe.kanada@atg.wa.gov or ben.carr@atg.wa.gov. For questions about the Task Force, please contact the Attorney General's Policy Team at policy team@atg.wa.gov.

Sincerely,

Fer

BOB FERGUSON Attorney General

Appendix 2: Marketplace Contacts

Amazon

- Amazon's ORC Engagement Team (ORCET) can be reached at LPOutreach@amazon.com.
- Law enforcement information requests can be submitted via a request tracker: https://ler.amazon.com/us.

eBay

- Victims can contact eBay's ORC team at proact@ebay.com.
- Law enforcement can contact the team at <u>lawenforcement@ebay.com</u> and submit requests to investigators on this portal: <u>https://le.corp.ebay.com/leportal_communitieslogin</u>.
- More information about working with eBay's Criminal & Regulatory Investigations Team: <u>https://pages.ebay.</u> <u>com/securitycenter/law_enforcement.html</u>.

Etsy

- Etsy's policy on requesting information about buyers and sellers: <u>https://www.etsy.com/legal/re-quests-for-information/</u>.
- Intellectual property owners can register their brands and report suspected violations here: <u>https://www.etsy.com/ipreporting</u>.

Mercari

Law enforcement can make requests online at: <u>https://www.mercari.com/us/help_center/topics/trust/poli-cies/requests-from-law-enforcement/</u>.

Meta

• Law enforcement can make requests online at: https://www.facebook.com/records/login/.

Nextdoor

- Law enforcement can make requests online at: <u>https://help.nextdoor.com/s/contactus?language=en_US&-subCat=Law%20enforcement%20inquiry&cat=Privacy%20and%20online%20safety.</u>
- More information about Nextdoor's law enforcement support: <u>https://help.nextdoor.com/s/article/Next-door-s-law-enforcement-support?language=en_US.</u>

OfferUp, Inc.

- Victims who believe that a prohibited item (including stolen goods) is on OfferUp can contact: <u>records@</u> offerup.com or use the process described here: <u>https://help.offerup.com/hc/en-us/articles/360032336271</u>.
- Law Enforcement agencies can also contact <u>records@offerup.com</u>. A page describing specific law enforcement resources, including how to use the LeadsOnline investigation system, can be found at <u>https:// help.offerup.com/hc/en-us/articles/360032336811-Law-Enforcementresources</u>.

Specialized ORC Team Interfacing with Law Enforcement:

OfferUp has an Investigations team that prevents and responds to criminal and fraudulent activity as soon as it is discovered. This team investigates suspicious activity and items and takes appropriate steps to intervene when risky behavior is identified. In addition to taking the appropriate steps to investigate and address issues that arise through the app, OfferUp partners closely with law enforcement, and encourages cross-functional team outreach between OfferUp, retailers, and law enforcement. Furthermore, OfferUp has established automated, proactive queues that can be supported with retail analytics as a result of having Organized Retail Crime and Retail partnerships.

OfferUp's <u>Law Enforcement Resources</u> webpage provides contact information to law enforcement agencies in North America seeking assistance and records for investigations relating to OfferUp. It also encourages law enforcement to take advantage of OfferUp's partnership with LeadsOnline as records are provided at no cost to their department and available 24/7/365. OfferUp users are directed to <u>Reporting a serious issue to OfferUp</u> where OfferUp encourages its users to contact local authorities if they have encountered illegal activity or a crime. The investigating officer may then contact OfferUp and OfferUp will work directly with the officer to help with the investigation.

Seller Vetting:

OfferUp uses a variety of verification methods for users on its platform, including email address, phone number, bank-level KYC verification for sellers who ship items through the app, and government-issued ID verification. Depending on circumstances, these methods can be voluntary or mandatory. Merchants who purchase OfferUp business services are verified through a validation of a business license. OfferUp also collects a variety of additional data types that it can disclose to law enforcement in the event of a crime or suspicious activity.

OfferUp INFORM Consumer Act About TruYou

Reports About Site Safety:

While OfferUp does not publish reports publicly, it leverages the best of machine learning, AI, and data analysis to proactively identify and remove content that is at risk of violating their counterfeit and stolen goods policies. In 2023, OfferUp received ~250K user generated reports from users who suspected items or accounts of being associated with stolen or counterfeit goods. Over that same period of time, OfferUp, used their user generated reports and full portfolio of detection capabilities to detect and remove roughly 1 million items and disable more than 10,000 accounts for risk of counterfeit and stolen goods.