Category / Specific items of compliance	Notes
Know Your Manufacturer’s Brand Protection Team	
Close coordination between secondary online marketplaces and manufacturer brand protection teams are key to patient safety and the securing of the supply chain.	Summary: You should have a way of allowing brand protection teams to contact you (phone and email) and receive an answer within two business days about suspicious products offered for sale. You should create accounts in ten business days for brand protection teams to do listing surveillance either through the standard interface or a brand portal. Bonus: You should provide an API for brand protection teams to pull listing data from.
Does the platform provide a portal through which brand protection teams can monitor	Providing a portal is the minimum level of compliance.
Have drug manufacturers that have requested logins on the platforms to monitor listings and	This will be confirmed with the brand protection teams and judged accordingly.
Does the secondary marketplace have an email address and a phone number for registered	Should we provide some guidance about how to signify a suspicious sale? Sometimes this will be up to professional
Know Your Products	
Using GS1 and DSCSA standards can help prevent diverted or counterfeit product from being sold through platforms.	Summary to do for compliance: Each product listing should capture the four DSCSA package ids (GTIN, LOT, EXP, SN) and store them privately with the listing's buyer, seller, and prices for six years. Listings should be kept for this duration whether completed, unsold, or withdrawn. Unique package identifiers should be disclosed to purchaser at time of purchase for shipment arrival verification. Listing information, if not available via portal, should be disclosed to product manufacturer protection team upon request within ten business days. No products identified by lot or serial number in recalls should be allowed to be sold. Sales of products should generate a DSCSA-compliant transaction history, information, and statement and store it for six years.
Does the platform record the unique identifying information (GTIN, SN, EXP, LOT) for all	To ensure people don't sell multiple units under one serial #, a listing should require entry of the identifiers at listing
Are product listings including buyer, seller, and prices and the GS1 identifiers associated	
Does the platform allow the manufacturer's brand protection team to see the buyer, seller,	
Does the platform reveal the unique identifying information (GTIN, SN, EXP, LOT) for a	
Optional: Does the platform allow purchaser of the product to confirm receipt of the same	Yes, the idea is that a purchaser would verify the unique identifying information on receipt of the product. We can't
Does the platform generate a transaction history record as required by the GS1 standards,	
Does the platform generate a transaction statement as required by the GS1 standards,	
Does the platform generate a transaction information as required by the GS1 standards,	
Does the platform disallow sale of products from lots that have been announced in recalls and counterfeiting alerts from manufacturers or regulators?	
Know Your Customer	

Modern diversion and counterfeiting rings adopt and shed corporate shells frequently to avoid accountability after their crimes are discovered. Online secondary marketplaces can help deter this behavior through rigorous identification of participants.	Summary to do for compliance: Collect many official designations (NPI, GLN, NCPDP, license #'s, etc) at registration time. Have and follow a documented Know Your Customer program. Verify that businesses are in good standing and have active bank accounts registered to an appropriate entity.
Do the platform's terms and conditions require that that registered entities on the platform	
Does the platform require all participants registered on the platform to provide their unique	
Does the platform capture a participant's NPI number at registration time?	
Does the platform capture a participant's state license and DEA license at registration time?	
Does the platform capture a participant's NCPDP number at registration time?	
Does the platform capture a participant's contact information, including phone number at	
Does the platform have a know your customer (KYC) program it follows? Is that program	
Does the platform verify that a business registered with the platform is in good standing with	
Does the platform verify that any bank accounts registered with the platform are open,	
Know Your Policies	
Clear, enforced policies can discourage bad actors from using a platform to sell dangerous medicine.	Summary to do for compliance: Ensure that terms of service / platform policies prohibit behavior that would endanger patient safety, so that violators can be banned from the platform, including: scraping GS1 product identifiers, being defendants in complaints related to supply chain safety or trademark infringement, failing to notify the platform that they are defendants in such cases, or failing to respond to platform or brand protection team inquiries about listings.
Does the Terms Of Service for the platform prohibit participants from scraping, downloading	Can be used as a basis for termination from the platform.
Does the platform state clearly in its policies that participants named as defendants in	
Does the platform's terms and conditions require platform buyers and sellers to notify the	
Does the platform notify participants of its policies and that it monitors the site for suspicious	
Does the platform have a policy that requires participants to respond to inquiries about	
Does the platform adhere to the following IT security	
The marketplace must adhere to current, relevant IT security standards to prevent bad actors from infiltrating the platform or using DSCSA information for unauthorized purposes.	Summary to do for compliance: Does the platform adhere to a number of IT security practices listed below? Does the platform have an external verifier of their security adherence, such as a third party audit or certification?
Uses HTTPS for all production web interfaces.	
Requires secure user authentication to access all web interfaces capable of conducting	

Requires individual user accounts and prohibits sharing of accounts between individuals.	
Associates individual user accounts with licensed and registered entities.	
Requires API keys for all third-party access to APIs that contain listing information and/or	Only if you offer APIs.
Can demonstrate external verification that the marketplace and IT systems holding sensitive	