

New smartphone technology tested at US Customs could ID counterfeits in “seconds”

Gemma Bradley

04 December 2025



Adam McCullough/Shutterstock

- **New technology donated to US Customs consolidates existing counterfeit detection software on one smartphone**
- **Customs officers can scan products to identify counterfeits in “seconds”**
- **Developers hope technology can be rolled out across US ports and internationally post-testing**

New smartphone software tested at JFK Airport could allow US Customs to determine whether a product is counterfeit in “two to three seconds”, according to its manufacturers.

[One Device](#), an integrated mobile platform donated by the [Alliance for Gray Market and Counterfeit Abatement](#) (AGMA), consolidates members’ brand-verification tools into a single device for Customs to use.

The first training session for the device – which aims to assist US Customs and Border Protection (CBP) officers to assess the authenticity of AGMA members’ products entering the US – took place in November at JFK Airport.

Only four phones were involved in the “classroom” training exercise. Around 30-40 CBP officials used the device on sampled goods, and feedback was positive, according to Ryan Smaglik, AGMA board member and director, revenue and brand protection at Rockwell Automation.

Who is involved?

AGMA created the software in partnership with [True Pedigree](#), a technology provider of data-driven brand protection software.

The One Device technology, platform, equipment and services were then donated at no cost to the CBP under the [Donations Acceptance Programme](#) (DAP), a partnership mechanism to collaboratively explore and implement tangible solutions to trade and travel facilitation and enforcement challenges.

Under DAP, CBP can accept donated technology, equipment, services and infrastructure from private companies and industry partners.

This allows CBP to “integrate cutting-edge technologies directly into frontline operations to better detect risks such as counterfeit products, fraud and other supply chain threats”, explains Shelley Raina, CEO of True Pedigree.

How does it work?

The One Device cloud-based platform delivers “fast, secure and reliable product authentication for multiple brands using a single device”, Raina says.

Historically, CBP officers have relied on individual guidance and/or technology from individual manufacturers and brand owners to identify counterfeiters. This can range from printed customs manuals to separate authentication tools on smartphones.

As a result, any number of smartphones and verification devices must be held at Customs and used individually depending on the goods, Smaglik explains.

This makes verification “slow, inconsistent and cumbersome”, Raina claims. Therefore, True Pedigree’s aim was to “leverage data and infrastructure” to make identification more “reliable and efficient”.

Every product has a label that contains multiple data points, Raina observes. For example, items will have a product serial number or stock keeping unit (SKU) – a unique alphanumeric code assigned to every product for businesses to internally identify and track items.

These data points can also include the manufacturing date and location, or product expiration date.

All of this information creates a “unique digital fingerprint” for the item, Raina says. One Device then analyses and validates that digital fingerprint in real time, he explains.

“For a Customs officer to authenticate a product, they simply take the One Device, hover it over the label or packaging, then the platform processes the embedded data and confirms authenticity in two to three seconds,” he states.

The scanned data is compared to information previously provided by brand owners, to determine whether the product is authentic.

If an anomaly is found between the data on the product and the data on the cloud database of brand information, then it is “more likely a counterfeit”, Raina concludes.

The smartphone is remotely managed and locked down in a so-called “kiosk mode”, Smaglik adds, to prevent misuse.

A closed system

According to US customs rules, when a shipment containing suspected counterfeit goods is stopped at the border, the importer has seven business days to provide proof that the goods are not counterfeit.

During this time, only limited information about the imported products (eg, a redacted image of the goods) can be provided to the trademark owner.

This limited information can make it difficult for trademark owners to confirm the authenticity of goods and can delay the enforcement process until either the importer has responded or seven days have passed.

If the importer does not respond in the time frame or provides insufficient proof that the goods are not counterfeit, CBP may then release additional information, including unredacted images of the goods, to the trademark owner, which can then take action against the importer.

To help prevent delays in this process, the One Device technology uses a so-called ‘closed system’, in which True Pedigree acts as a “middle party”, Raina explains.

True Pedigree has “agreements in place”, allowing it to see information that would be otherwise unavailable, during the seven-day grace period. This allows the company to determine whether items are counterfeit quicker.

“That's why companies are selecting us,” Raina concludes. “We kind of become that intermediary body that dictates how the information flows.”

The role of AI

AI LLMs are not directly used on One Device, but they have been used by True Pedigree in developing individual brand protection apps, Raina explains.

For some of the brands that feature on One Device, True Pedigree has also developed an initial authentication application, which has been added to the smartphone.

“The One Device is bringing all of these applications to get it into a centralised platform and the individual applications are also in many cases built by us,” Raina explains.

Where relevant, machine learning and AI has been leveraged in this development process, “to be able to detect anomalies either on the package or the label itself” of potentially counterfeit products, Raina says.

Incorrect font sizes or spelling mistakes, as well as any other anomalies on the product, are analysed using AI to determine a “risk score” for each item, Raina says.

Some of these apps have already been uploaded to One Device; others will be soon.

What is next?

Only AGMA member companies – which include Cisco and HP, – are currently covered by the device. However, Smaglik hopes that the technology will appeal to more companies, as well as expanding into further US ports and eventually on an international scale.

“The same needs that US Customs has... are applicable anywhere else in the world,” he notes. Many AGMA members and brand owners are “doing business in more than one geography”, he says.

“We’ve only touched one port,” he admits. “We need to continue this roll out... in the United States, [and] work with Customs to refine the concepts, the management of the device, the support and all the realities on how to operationalise this,” he says.

It is unclear when the technology will be rolled out further, but Smaglik says that, in the US, it could be “any order of weeks”.

Raina hopes that the product will also be used in smaller mailing facilities (eg, FedEx or DHL facilities), where CBP officials are often onsite already.

“A lot of the counterfeit products that might come into the US do not come on big containers or pallets. They might come in small packages, especially pharmaceutical products,” Raina asserts.

He also wants to expand the technology internationally, including through donations to Europe, Africa and the Middle East.

“We hope that this opens up access, [and] puts the right tools, at the right time, in customs authorities’ hands again,” Smaglik concludes.

“That's our hope – that every brand doesn't have to go through and navigate this on their own and can come to one place and have a very efficient way of working through technology with customs authorities.”



Gemma Bradley

Senior Reporter

World Trademark Review

gemma.bradley@lbresearch.com

[View full biography](#)