Beyond the Image

Uncovering Coordinated Claims Fraud

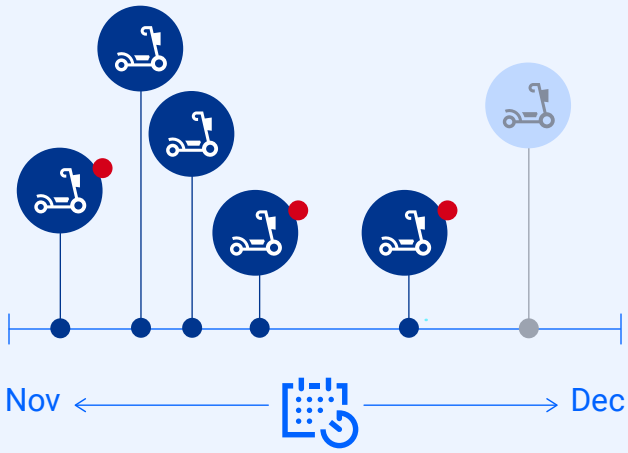
Verisk

Spotting the fake is just the start

When a claim professional catches a “borrowed,” doctored, or wholly fabricated photograph in a submission, it’s a small win in the fight against fraud. But identifying that photo may be only the start of unraveling a claim that’s inflated or entirely fictitious.

Claims submitted to 6 different carriers within 1 month

● claims with SIU involvement



Claims organizations grapple with a growing array of digital fraud, including repeatable, adaptable schemes that can be repurposed across multiple submissions and insurers, evolving to evade detection. Teams fighting today’s AI-enabled scams need AI-driven tools of their own.

Verisk’s AI-powered **Digital Media Forensics**, integrated with **ClaimSearch®**, can help peel back the layers of deception employed by fraud rings, and it can empower special investigation units (SIUs) to keep up as claimants add and subtract elements of their stories. Consider one type of fraudulent claim that’s multiplied and adapted of late: alleged crashes involving cars and e-scooters, e-bikes, or other property. A recent example shows how these fraudsters work and how an insurer can fight back.

The visual proof

At first glance, the evidence looked credible — photos of a damaged scooter, complete with a barcode label, serial number, and purchase receipt to support authenticity and value. But Digital Media Forensics revealed a different story. In this case, it matched the photos with online images the claimant downloaded. Upon being alerted to the re-used pictures, the claim was referred to SIU where investigators took a closer look and detected alterations to those photos, including subtle differences in the font and brightness of lettering where the fraudster doctored the serial number to change the date of manufacture. Separately, digital alterations to the receipt were found to obscure or modify key details to support the false claim.

original

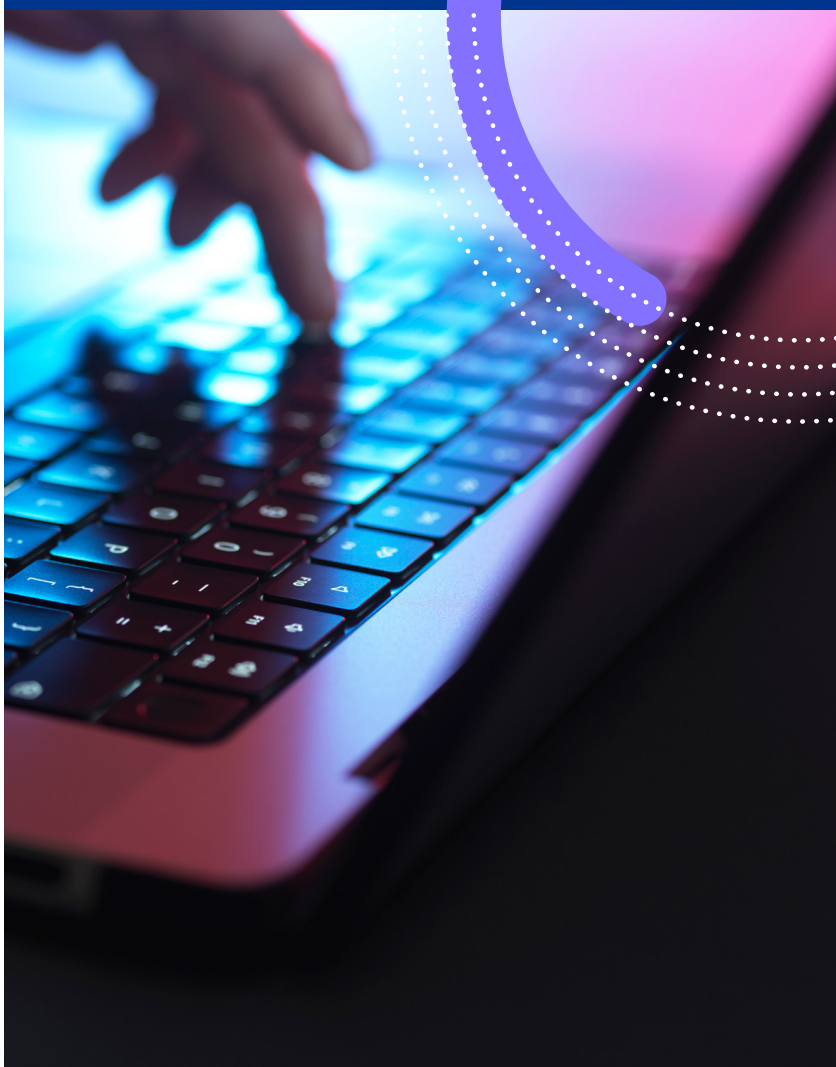
altered image

The claimant

These schemes often hinge on confusion about who the true victim is. In many cases, the legitimate policyholder is not the fraudster—but rather a victim of identity theft. Fraudsters take over an active, longstanding policy and submit a claim on behalf of that policyholder, banking on the insurer's trust in an established customer. To complete the scenario, they create a synthetic identity to serve as the "victim" in the claim, typically the alleged owner of damaged property such as an e-scooter, bicycle, mailbox, or fence. This blending of stolen and synthetic identities reflects how **digital deception is reshaping insurance risk**, allowing fraudsters to mask their activity behind otherwise credible claims.

In this case, the fraudster posed as the policyholder and admitted fault, claiming to have swerved to avoid an object in the road and instead struck another individual's scooter. That individual did not actually exist. Because the policyholder appeared cooperative and at fault, and because the claimed damage was relatively low value, the submission fit a familiar, low-friction pattern that often results in fast payment with minimal scrutiny.

Digital Media Forensics disrupted that pattern by revealing reused images, repeated narratives, and overlapping identity elements appearing across multiple claims and insurers. What initially appeared to be an isolated loss was exposed as a repeatable, scalable fraud scheme.



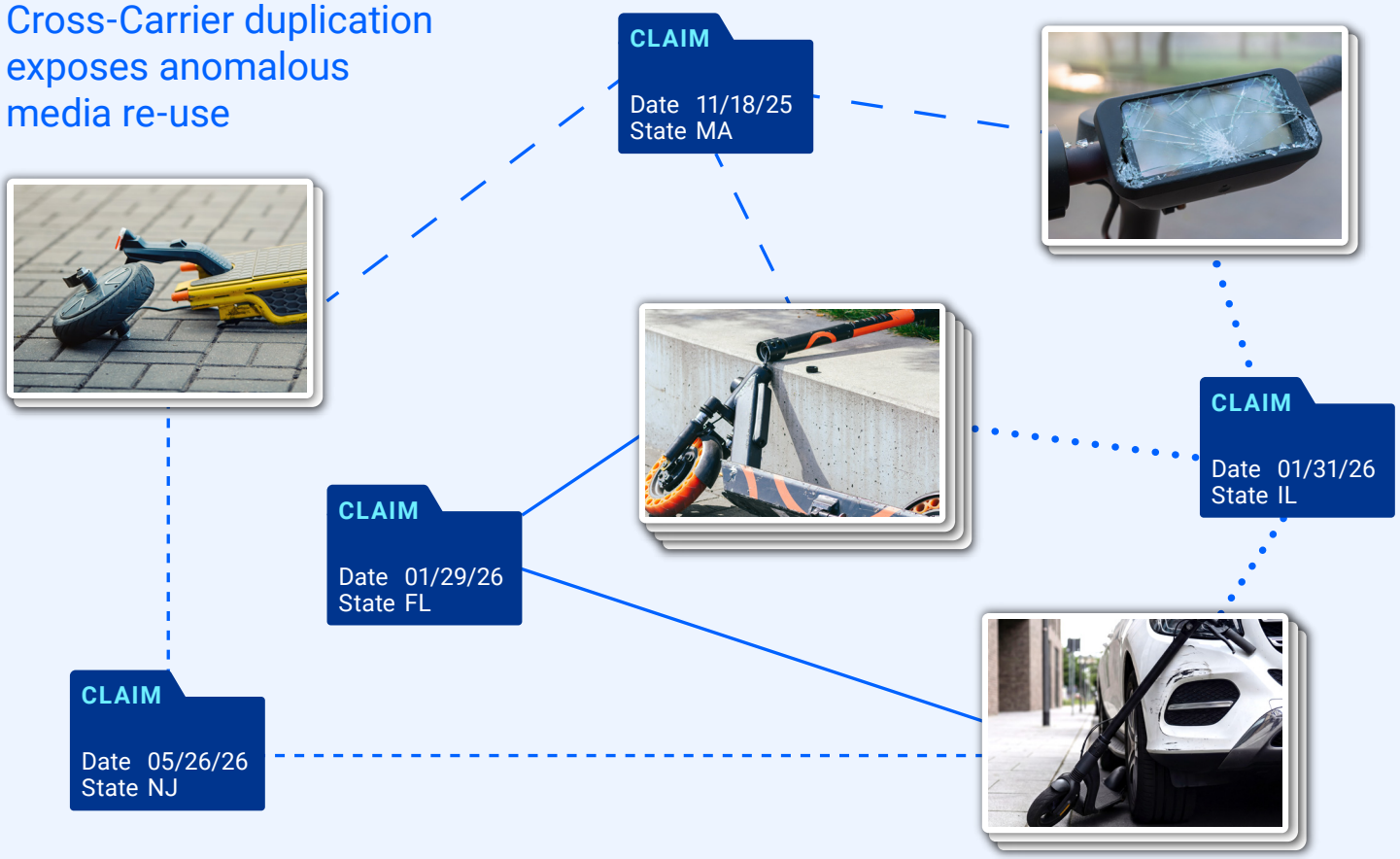
The network effect

When Digital Media Forensics and **Network Analysis** are combined, they can uncover patterns of fraud that can lead investigators beyond catching individual cases to cracking organized fraud networks. What began as a single scooter claim revealed a broader scheme spanning 13 states over 10 months, using 19 reused images and generating referrals to nine departments of insurance. The same narrative appeared in five states over five months, with the same person claiming damage to his scooter in three of those alleged incidents, occurring as little as two weeks apart.

Identifying these bad actors, along with the phone numbers and email addresses they use, adds to the library of information that claims and SIU staff can consult to flag potential fraud in the future and prevent unnecessary payouts.

The resourcefulness of fraudsters leaves little room for claims teams to relax. A detail of today's most prevalent scheme could change tomorrow: the e-scooter may become some other vehicle, or a pedestrian. The narrative of the collision may shift. Digital Media Forensics stands ready to adapt and keep users a step ahead.

Cross-Carrier duplication exposes anomalous media re-use



See how Digital Media Forensics can bring deeper, AI-augmented analytics to the fight against fraud.

Contact a Verisk representative.

Verisk