LUXURY WITHOUT COMPROMISE

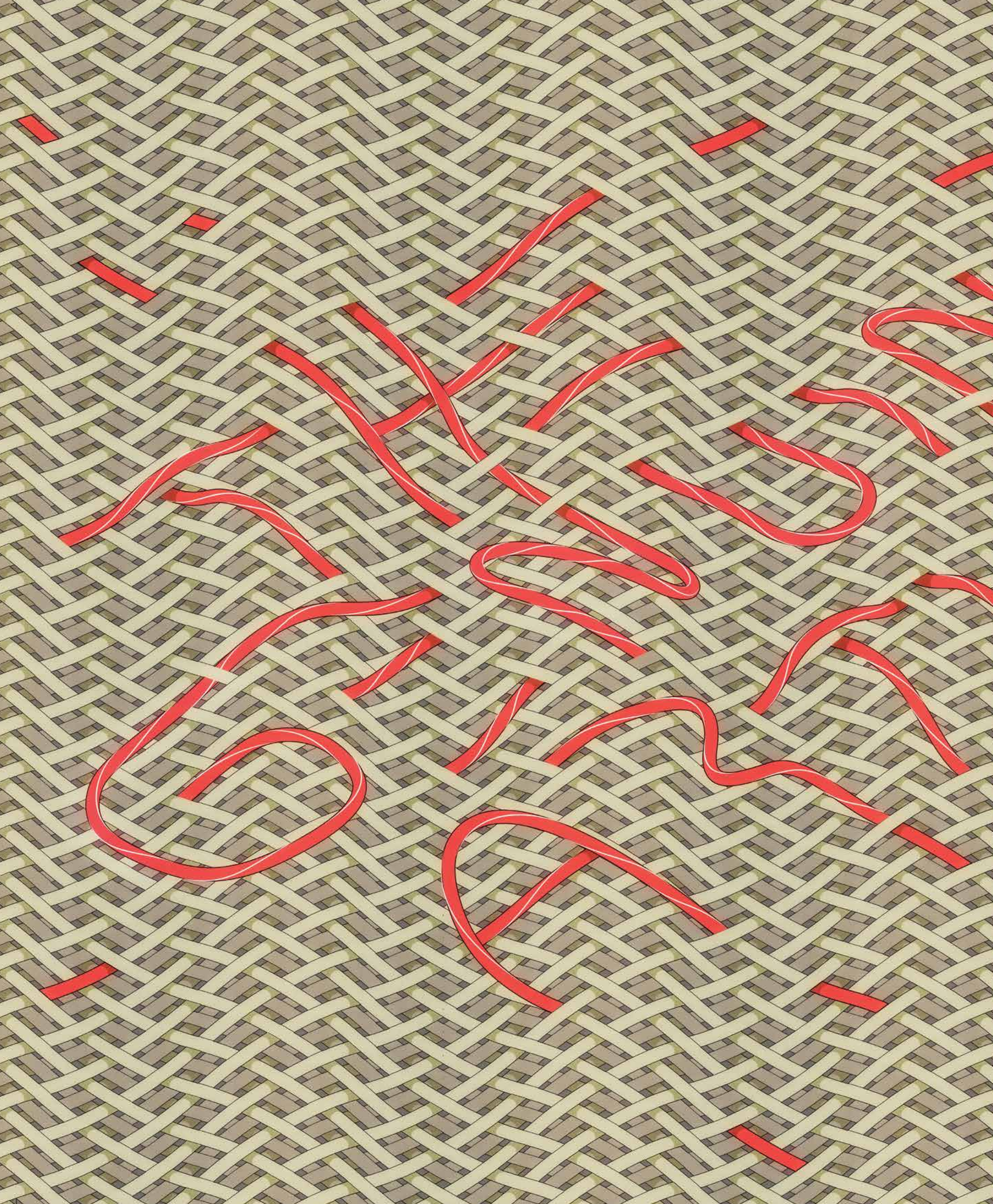
Robb Report

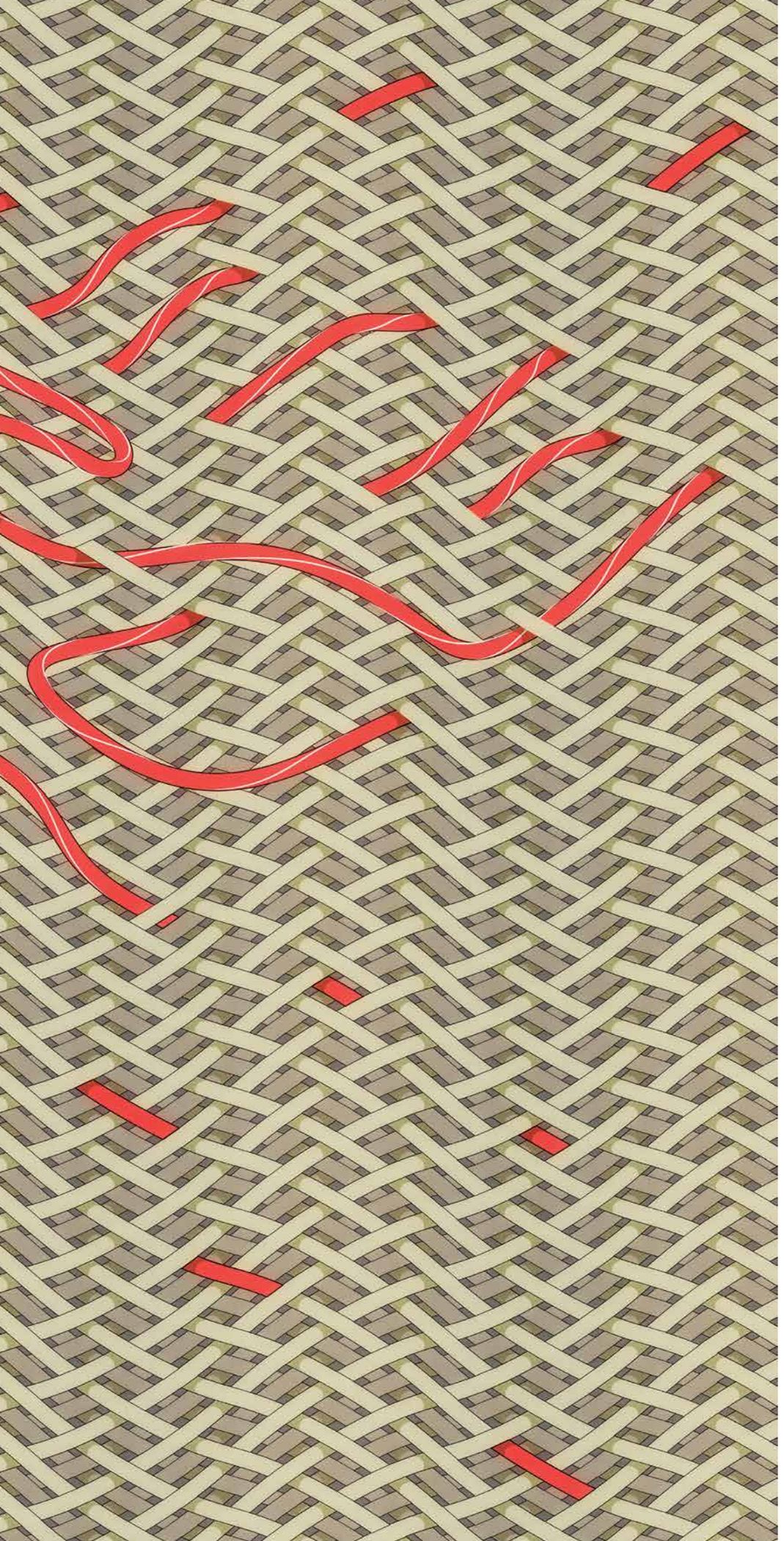
The FINISHING TOUCH

WATCHES AND JEWELRY ISSUE

ASTUTE INVESTMENTS
IN TIME & BEAUTY

NOVEMBER 2018





Here Come the Fraudbusters

Counterfeit goods cost the luxury industry billions a year. Now they're fighting back with radical technology—and some shellfish.

BY
MARK ELLWOOD

ILLUSTRATION BY
CHARLES WILLIAMS

On a remote Mongolian hillside, bells tinkle in the distance—a sign that a herd of cashmere-producing goats is nearby. A woman follows the noise, picking over the rocky terrain with a small canister tucked under an arm. In just minutes, she has crouched down and sprayed the underbelly of each animal, leaving no residue; indeed, there's no evidence she was ever there.

Fast-forward a few months to a boutique on Rodeo Drive in Beverly Hills, where a sales associate passes a cashmere sweater over a scanner attached to the register. It displays the date and location that the cashmere was marked that morning in Mongolia along with the factory where the wool was processed and even the date the sweater arrived stateside. "We use synthetic DNA to guarantee the provenance and quality of the garment," she tells a customer, offering to play a video of its origins on that mountainside.

It's futuristic, perhaps, but trials of this process—where premium raw materials are marked at the source with an indelible, invisible tracker—are already underway. It's just one of the high-tech ways the luxury sector is fighting back against the ever-increasing boom in fakes.

Counterfeiting remains one of the world's most lucrative ways to break the law. Already worth almost $500 billion annually, per the Paris-based Organisation for Economic Co-operation and Development, it's predicted to reach a staggering $2.3 trillion by 2022; the World Customs Organization believes that seven percent of all global trade is in fakes. This surge is largely a by-product of the 2008 economic crisis when many consumers who had a healthy appetite for luxury goods had to tighten their belts—from cautious Americans to ruble-toting Russians who've seen their spending power torpedoed as the currency cratered.

It provided the perfect conditions for a boon in fakes. Simultaneously, supply chains have grown less reliable: Overseas, lower cost production with less scrupulous oversight allows leakage and extra shifts in the same factories. Added to this, the boom in e-commerce has created a new platform on which to sell those counterfeits, often unchecked.

Apparel brands alone spent $6.15 billion last year on their efforts to fight fraud, and other sectors, from art to wine, spent billions more. Much of that money was allocated to discreet new ways to protect their brand equity and reassure their loyal customers, like the science used in that cashmere sweater.

Entrupy's anti-counterfeiting hardware and smartphone app determine whether a product is authentic or "unidentified."

Stefano Ricci embeds radio-frequency identification (RFID) chips in its products to keep track of inventory.

New York-based Entrupy's new anti-counterfeiting system relies entirely on AI via a handy little gizmo.

The company behind the DNA science is Stony Brook, N.Y.–based Applied DNA Sciences, which can apply its synthetic DNA molecules to almost any surface, says MeiLin Wan, vice president of textile sales for the firm. A unique sequence is created for each customer and is held in its database; against it any product can be subsequently tested. Currently, the system involves swabbing a product with a Q-tip and then sequencing the solution in a machine or dabbing it onto a solution that will glow red if synthetic DNA is present. The firm aims, though, to create near-instant scanning, like the device in that futuristic Rodeo Drive boutique.

It's virtually impossible, Wan explains, to remove, transfer, or replicate the DNA outside the firm's labs, as the Department of Defense—another client—found firsthand. Its scientists tried, unsuccessfully, for more than a year to either re-engineer it or move the DNA to another surface. For firms in the luxury sector, Wan continues, the compelling use for this technology lies in policing and controlling supply chains.

Many luxury firms that use DNA tracking also safeguard their product with more analog methods like those developed by OpSec Security, a British firm with offices across the world. "We're all chasing the silver bullet of authentication, and combining the physical and the digital gets us one step closer," says Bill Patterson, OpSec's vice president of global marketing. His firm offers a series of near-invisible techniques for additional reassurance, in the supply chain or at retail. Take any clothing item—a trench coat, perhaps—and look closer. The care tag might incorporate a seemingly random number sequence that is, in fact, a serial number, or a piece of fabric might be sewn into the seams that you can remove only if you know where to look, and unpick it in the right place.

Then there's microthread, an ultrafine nylon or plastic twine sewn into the garment, featuring images or phrases that can be spotted only under a magnifying glass. It could be the brand's logo or something more creative—an insulting phrase, for instance, like the high-fashion firm that chose to point out how only pirates and prostitutes loved counterfeit goods.

Of course, such technology is only watertight once the entire luxury sector adopts it as standard. Until then, verifying authenticity further down the supply chain is vital; the newest tool on this front is AI, or machine learning. New York–based Entrupy's new anti-counterfeiting system relies entirely on AI via a handy little gizmo that the company's Devin Battersby, Entrupy's customer-support lead, demonstrated for *Robb Report*.

Entrupy's hardware consists of a magnifying lens clamped to the back of a smartphone, which pairs with its own app. Battersby snaps it onto a handset before wielding the device over a pair of seemingly identical purses. The app prompts her to snap several pictures of specific angles—with the logo, fabric lining, exterior stitching, and the like—and she hits submit. The results for each bag are different, though. After a few seconds, the product is either deemed AUTHENTIC, complete with a check mark,

or, sadly, flagged as UNIDENTIFIED. It's Entrupy's euphemism for a fake.

The system is ingeniously designed. Those images Battersby took were uploaded to Entrupy's master database at a magnification of 260 times the naked eye. Its proprietary algorithms then cross-referenced them with its in-house archive of more than 50 million photos of some 60,000 unique items dating back 80 years. Near-instantly, then, it could offer that verdict.

What's more, the AI's performance improves as it gains customers and data. Each scan adds momentum: When the firm first tested the system two years ago, its accuracy reached around 94 percent. Today, cofounder Vidyuth Srinivasan says it's at 99.1 percent. He's so confident in Entrupy's system that there's a money-back guarantee. "There's a process to follow then, and if we're proven incorrect at the end, we'll happily buy the item off you, repaying you what you had to pay for it," says Srinivasan. So far, that's happened just 20 times in the firm's history; compare that with the $70 million worth of goods it has successfully authenticated.

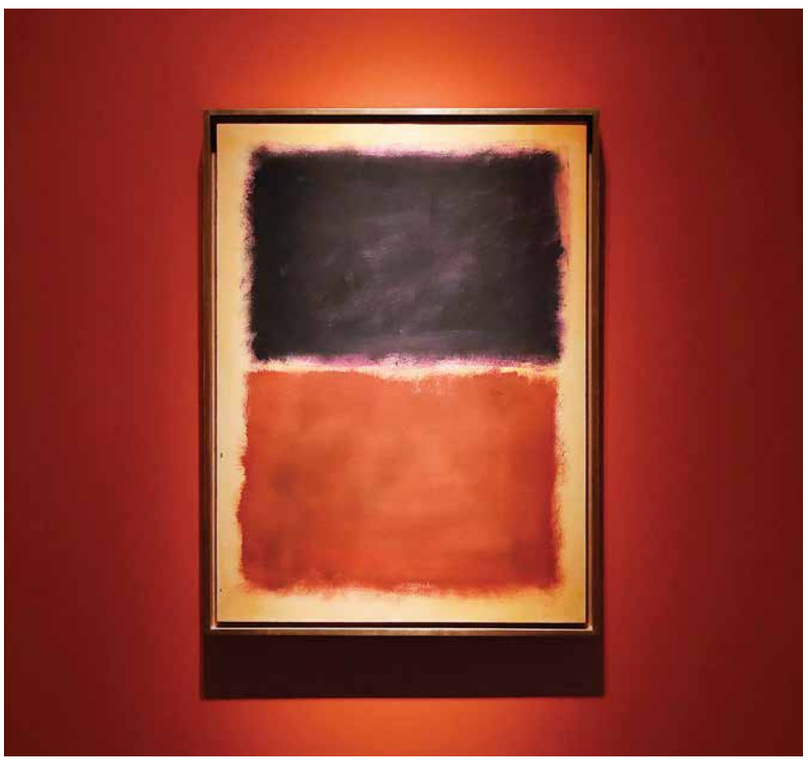
It now has more than 300 paying customers (the device is leased for $299, and the monthly subscription service starts at $99). These include consignment stores as well as luxury online resellers, the booming sector featuring the likes of the RealReal or Material World. Entrupy launched with a focus on handbags, as these are the most commonly counterfeited items, but it will soon expand to shoes and high-end sneakers. It's harder for its technology to work on high-reflective surfaces without texture, though, so it can't be applied to diamonds, glass, or porcelain. Verifying the authenticity of timepieces requires an entirely different approach, as Vintage Caliber's Simon Stern explains—one that sometimes involves a Geiger meter.

As one of Europe's top secondhand watch dealers, Stern is fastidious in detecting fakes. Early luminous watches contain small amounts of radium to help them glow, a practice long outlawed for safety reasons, and Stern uses this as his first test. Swiping a basic Geiger counter over a timepiece that claims to date back earlier than the 1960s will verify the presence of true radioactivity, which was outlawed in manufacturing after that date.

Another technique requires that he shine a UV light over the dial in a darkened room. Radium is not only a durable element but also an aggressive one, degrading the sulfides that produce the glow over decades; the result is that timepieces' luminescence dwindles as they age. "The lume should be very reactive but fade away immediately," he notes. "If it stays luminous for minutes, that's a clear indication of restoration or imitation."

When Stern has doubts about non-luminous watches, there's always non-destructive spectral analysis, which will break down the chemical content of the metal alloy used in a given timepiece or the paint compound used on the dial. Each is unique to a given manufacturer, of course, and so can be cross-checked with a verified model. Indeed, manufacturers are so keen to stymie future fakes that they're changing the raw materials they work with. Witness the rise of exotic, hard-to-source tantalum-tungsten alloy, which is fiendishly hard to machine without expertise. Likewise, replicating Hublot's ceramic and carbon-fiber models is possible but too expensive to be cost-effective for the counterfeiters.

The potential windfall from a fake artwork is sizeable enough to justify painstaking forgeries.



A faux Rothko piece displayed at *Treasures on Trial: The Art and Science of Detecting Fakes* at the Winterthur Museum in Wilmington, Del.

AP/SHUTTERSTOCK

The potential windfall from a fake artwork, though, is sizeable enough to justify painstaking forgeries. It's no wonder, then, that the art world is among the luxury sector's most fake-prone fields. See the downfall of New York's storied, 165-year-old Knoedler gallery, which closed in 2011 amid a deluge of lawsuits over whether it knowingly, or inadvertently, sold millions of dollars' worth of fake Rothkos and Jackson Pollocks. That $80 million scam, the largest in American history, was only unearthed thanks to the painstaking detective work of fraudbuster Jamie Martin. Tasked with verifying one of the newly discovered Pollocks that Knoedler had touted as genuine, he used a stereomicroscope to spot that the signature was traced with a needle.

What's more, the paint on the canvas included Red 170, a pigment that was only widely available years after Pollock died in a car crash. In the wake of this exposé, Martin's expertise earned him a new role, as Sotheby's in-house director of scientific research. Knoedler should have hired Martin before one of its unhappy buyers did, instead of trusting expertise alone—after all, if attribution is a human process, it's all too vulnerable to our limitations. And that's where Artendex believes it has the answer.

LISOVSKAYA NATALIA/SHUTTERSOTCK

Food is not immune to fraud. These French oysters are etched with the Gillardeau logo and followed along their distribution route via a hidden tracking device.

If only the walls of those galleries could talk, and if radio-frequency identification (RFID) and near-field communication (NFC) chips had existed hundreds of years ago, they just might. These microchips can be discreetly embedded in almost anything and used for tracking and monitoring. Early adopters—including fashion brands Moncler, Ferragamo, and, most famously, Burberry—have been experimenting with them for some years.

When Burberry's splashy London flagship opened six years ago, customers could wave garments tagged with RFID chips in front of screens to learn more about how they were made.

Stefano Ricci has taken this technology further: It started including RFID chips in its core items, mostly leather goods, four years ago. "It proved a great success in both speeding up the logistics process and making it safer and more accurate, since we could keep track of inventory," says the firm's CEO Niccolo Ricci. Now, Ricci has moved to add NFC chips, the same technology used by the likes of Apple Pay, as well. These can be read using any contemporary smartphone—just wave it in front of a Ricci-branded item with the right app installed, and there's instant reassurance the product is genuine.

It's the same technology that high-end Napa Valley winemaker Opus One has employed for 10 years. CEO David Pearson says he's "very satisfied" with the results, as complaints of fakes have plummeted since the NFC began; they now remain at or near zero. Scanning the chips on Pearson's bottles not only offers reassurance but also launches a short video of the winemaker. Opus One notes that actual scans each year remain rare. He likens his NFC process to a private security service in your home. "People might drive by once or twice a night," he says, "but it's the sign in the yard saying you're protected that [matters]. People know you're watching."

Then again, sometimes it's useful to make security measures both evident and invisible, as Gillardeau found out. This family-run fourth-generation firm from western France produces the world's most prized oysters. Each year, 2,000 tons of its spéciales, plump and nutty, arrive in restaurants, often costing $11 each or more. Unsurprisingly, this makes Gillardeau's products prone to counterfeiting and theft.

Four years ago, after a flood of such problems, the family invested millions in a laser that etches its signature logo onto every oyster without breaking the shell or affecting the taste. It also turned to Olivier Descoubes, a local entrepreneur who had watched the problems accelerate—one producer in Mont-Saint-Michel, he learned, had lost 130 tons of bivalves.

Descoubes responded with a cunning, but simple, invention: a tracking device disguised in an empty oyster shell. Gillardeau invested heavily in his $185 gadgets so it could track those oysters from farm to table. Descoubes's firms take empty Gillardeau shells and install a low-power homing beacon in each. "The hardest part was molding the resin to cover all the electronics so it's waterproof," he says. "But now we have a secure, robust product." With this and other tech, fraud will be reduced to just another easily spotted shell game.

Descoubes's firms take empty Gillardeau shells and install a low-power homing beacon in each, the seafood answer to a Trojan horse.

Another AI-powered start-up is Artendex, which collaborated with Netherlands-based Atelier on the Restoration & Research of Paintings project led by professor and AI expert Ahmed Elgammal. He says the challenge isn't just the unreliability of human know-how, but also that the techniques Martin employed share a common flaw. "The different technologies for detecting forgery in art attribution all depend on the physical property of the art: the canvas, the pigment, chemical analysis via X-ray," Elgammal explains. Why not instead look at the strokes on the canvas, as unique to each artist as their signature?

Elgammal helped develop an algorithm to do just that. First, the system scanned 300 line drawings by the likes of Picasso, Matisse, and Schiele before a deep recurrent neural network began crawling over those same scans, learning the characteristics of each artist's strokes. Then the team tested it using images it knew to be both fakes and authentic; in initial trials, Artendex's AI had an 85 percent accuracy rate.

Now, looking to commercialize this service, Elgammal is working on refining the analysis of drawings via art-world partners supplying further samples for the master database. He also wants to move into other areas, like paintings, though the professor admits that it's a dauntingly large undertaking to tackle. "It's because the strokes are not necessarily visible; it all depends on the art movement. In impressionism, you see them very clearly, but in old masters, you can hardly see the strokes."