The Top 7 THREATS to Authenticity

And the printable defense tactics you can offer

<Intro>

The year is 2019. The scene of the crime is anywhere. And the potential victim is anything or anyone, at any time of day. No consumer is safe. No brand out of reach.

Between the internet and sprawling global economy, the world today – while better connected and bursting with opportunity – is full of dark menaces, from phishing scams to full-fledged identity theft.

But it's not just our identity or confidence in $100 bills that are at risk. It's an endless array of products threatened by counterfeiting, misappropriated use, or outright theft. From cosmetics, alcohol, and food, to concert tickets, lottery cards, and even agricultural commodities like pesticides and seeds, brands and organizations in every sector are under attack. Worldwide losses are estimated at close to half a billion dollars annually,[1] and edge into the trillions when you add public safety damage to the equation.

As individuals and print and packaging professionals, it's up to us to help keep ourselves and our customers safe.

This eBook provides an overview of the most pressing threats to identity and security, escalated by a digital world. It also shows how, with the help of anti-counterfeiting and security printing technologies, print and packaging suppliers can effectively protect their customers from all sorts of hazards. It's about ripping off the mask of hidden dangers to take back control, beat back revenue loss, safeguard identity, and ensure product authenticity.

#01 The Dark Web

#02 Counterfeit Consumer Goods

#03 Brand Piracy

#04 Gray Market Diversion

#05 Identity Theft

#06 Activist Attacks

#07 The E-Commerce Effect

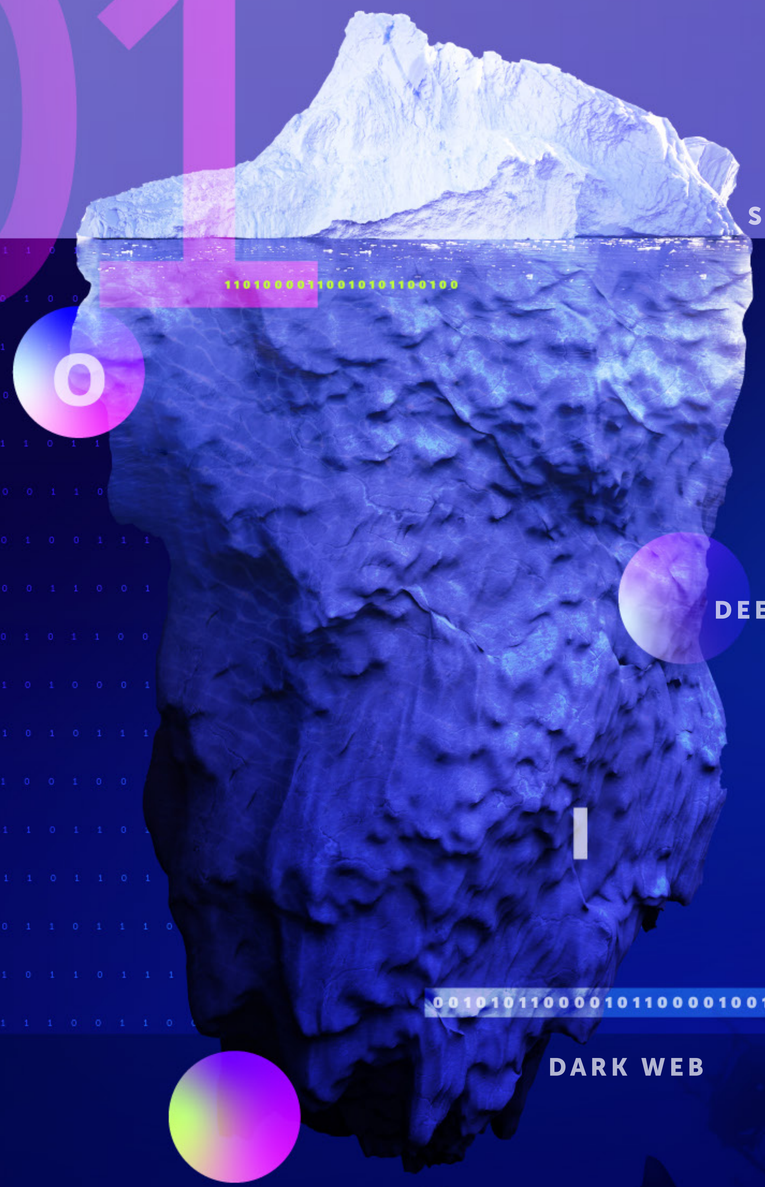
[1] The Future of Anti-Counterfeiting, Brand Protection and Security Packaging to 2022, Smithers Pira, 2017

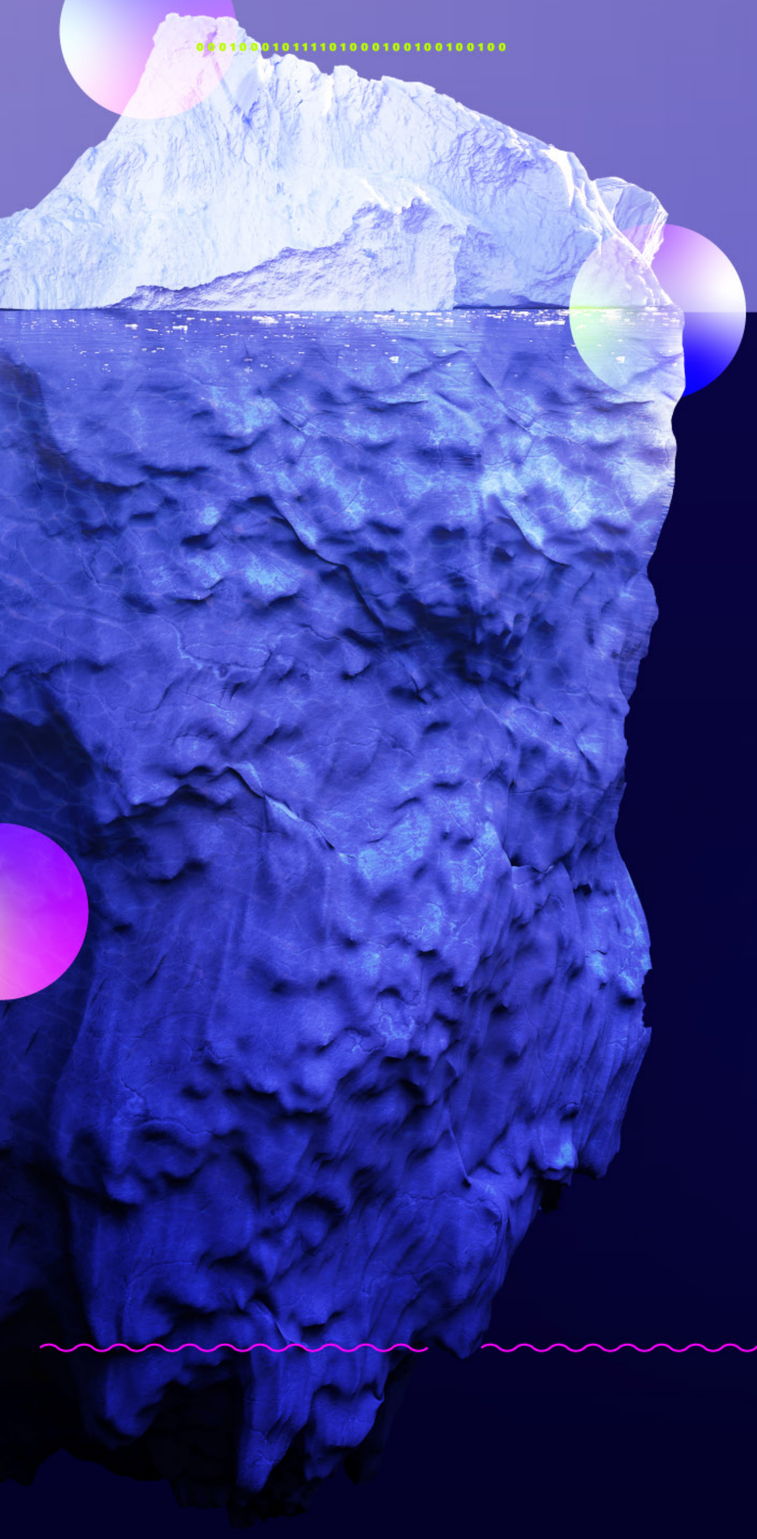
01

The Dark Web>

Many of us think the World Wide Web consists of those easily accessible sites everyone visits to search and browse, like Google, YouTube, and Wikipedia. But, that's just the surface.

Right below is the Deep Web, with its password protected access, like online banking, video on demand, or government databases.





Diving down further, there's the Dark Web, where domain addresses end in ".onion". In its murky waters, reached through the web-browser Tor, visitors are left as they wish to be – anonymous and untraceable, hiding both identity and location.

The Dark Web is widely used in the illegal underworld, and it's not recommended to buy products there. But it's also known as a secure place heavily backed by US government bodies to support all sorts of vital activities. Examples include whistleblowing sites, resources for those fleeing domestic violence, SecureDrops for anonymous tips to journalists (think WikiLeaks), and political forums for people living under oppressive regimes (such as during the Arab Spring). It's even home to a whole range of more mundane pursuits, from social networking, to online chess clubs, album releases, and even bake sales.

It's a constant race to keep the evil players from taking over, and stop illicit activities from overshadowing the forces of good. Hence, with all that anonymity, the question remains: what can we do to keep people and products safe along the way?

Outpace The Dark Side

By frequently innovating and changing security features, HP Indigo offers a diverse range of dynamic security solutions that help you stay ahead of threats to product legitimacy. Empowered by the agility high-quality digital print provides to create variable data, serialization and multi-layer security features – all in one on-press production process – you're better able to protect product authenticity every step of the way.

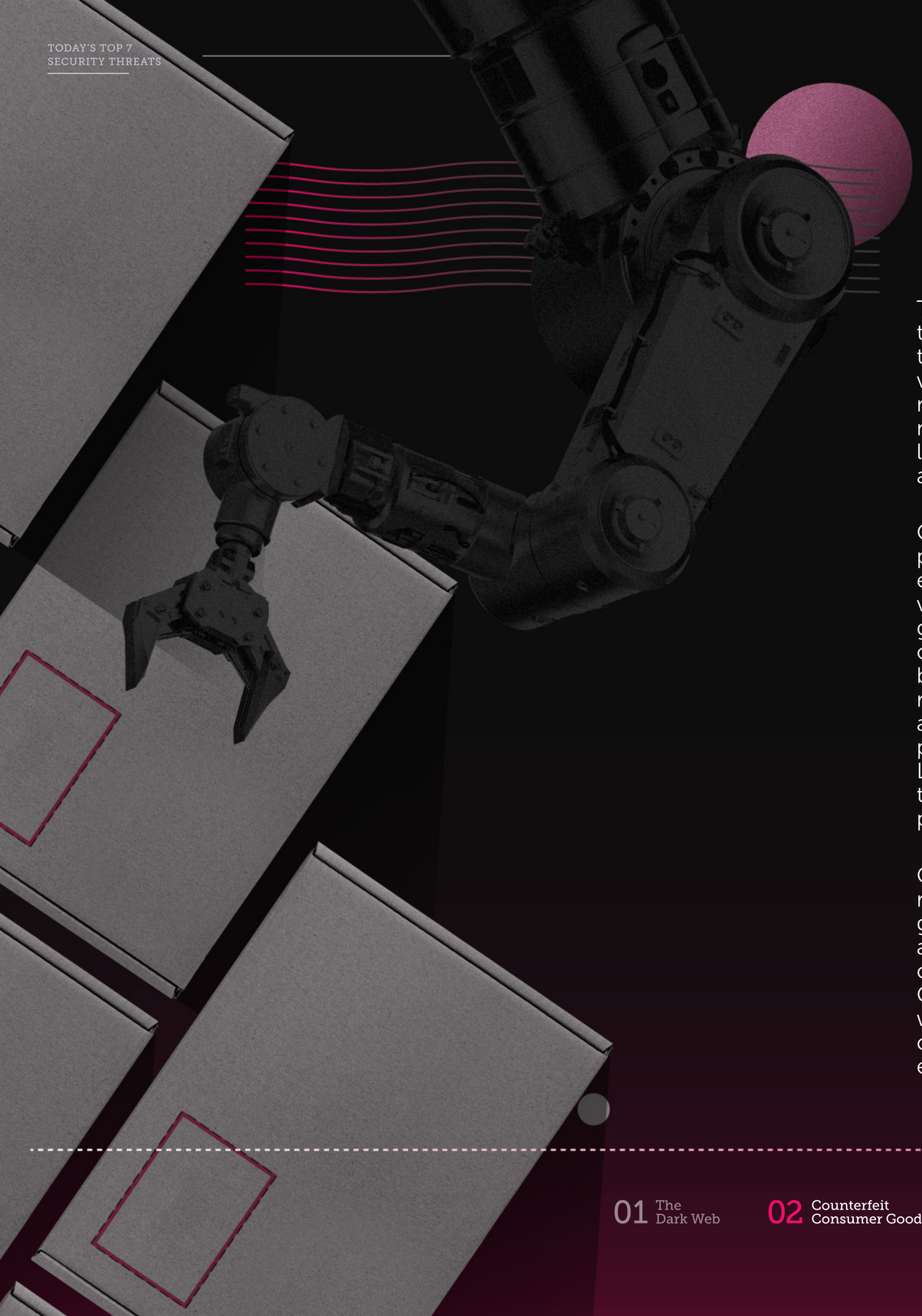
02

Counterfeit Consumer Goods>

Counterfeiting involves the manufacturing or distribution of goods using somebody else's name, usually at a lesser quality, and without their permission. For brands and other businesses, you might say it's a crime similar to identity theft.

In 2013 alone, the OECD estimated that about 5% of the goods imported to the European Union were fakes. In less-developed countries, the problem is even more severe. And no industry is safe.

You'd be amazed, but just about anything and everything can be counterfeited these days, from vodka to postage stamps and food vouchers, to ginseng, medicines, music, and face cream.



There are a lot of negative effects to all this counterfeiting. Often, consumers who think they are purchasing a discounted version of a brand name, are actually receiving a subpar product. It can even be more dubious than that, supporting child labor, organized crime, and costing cities and countries valuable tax revenues.

Of course, it also hurts brands. Besides the potential harm to a brand's reputation, it's extremely costly to business. According to various studies, counterfeiting has been growing at a rate of more than 10,000% over the past two decades, stealing $460 billion from brands each year. The damage reaches the trillions of dollars mark when accounting for all forms, from software piracy to trade secrets and copyright theft. Lost sales mean lost profits, which in turn translate to lost jobs for workers and higher prices for customers.

Consumers can make better choices by refusing to pay a price that looks "too good to be true". They can also pay attention to the packaging, which in counterfeited products is often shoddy. On the manufacturer's side, there are ways to protect their products that make counterfeiting efforts too complicated and expensive to be worthwhile.

Verify Product Authenticity

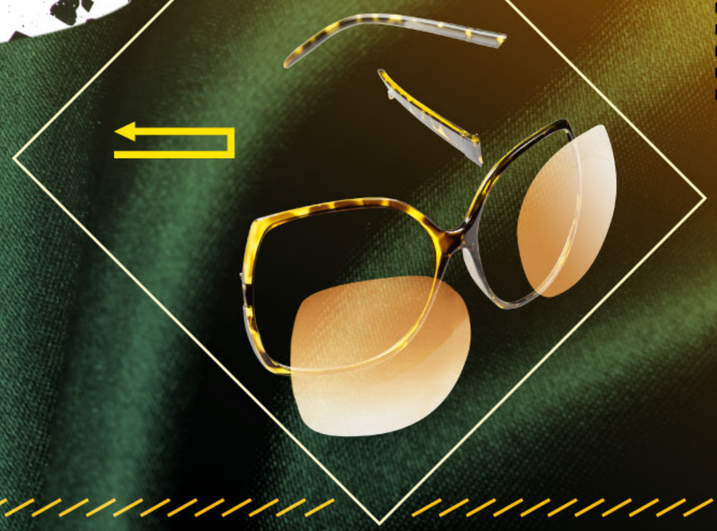
HP Indigo security and brand protection solutions provide irrefutable forensic authentication elements. Using security taggant inks which are only visible in specific light waves, documents, packaging, and the entire product supply chain are better protected. These authentication elements provide hard proof when there are disputes concerning counterfeit products.

Brand Piracy >

Ahoy there! Today's seas may be mostly free of swashbuckling pirates, but in business, piracy continues to be a very real threat – in the form of brand piracy.

Basically, there are four ways perpetrators take consumers and their brands captive in this sketchy pursuit.

The first is the world of knockoffs. Unlike counterfeits, which are meant to clone the original product, knockoffs come with names or logos similar enough to the original to be recognized by consumers. Just change a letter from Nike to Vike, and you get the drift.



In some cases, it could even be the exact same product, created in the original's factory, with the workers running an extra shift to produce a differently labeled version.

Or, the knockoff product may simply imitate the physical appearance of the original product, without a label, like a look-alike Louis Vuitton bag purchased on a street corner. Whichever the case, there may be legal implications if proven that the product was designed to confuse consumers.

Then there's what's called reverse engineering. With a little study and research, modern-day pirates deconstruct the brand's product to find out what it's made of – identifying all of its internal elements and ingredients, then replicating it to be sold at significantly lower prices. This is most common in the electronics industry, but also occurs with pharmaceuticals, pesticides, and agriculture fertilizers. Sometimes the quantities are off; other times the components or ingredients used are lower-quality than what the brand uses. In such instances reverse engineering is more than simply costly to brands, it can be dangerous to human and animal life.

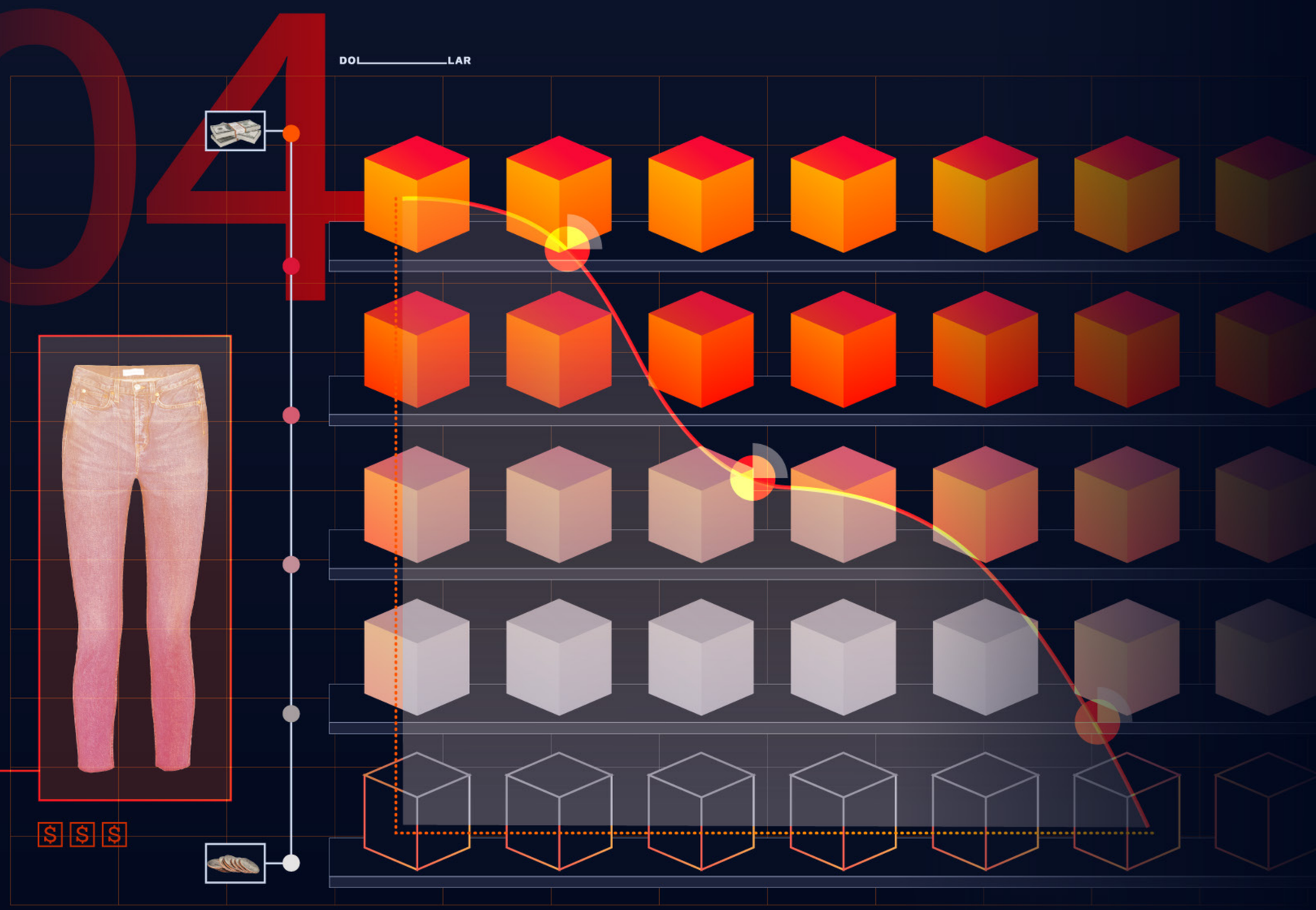
Stop Piracy Before It Sets Sail

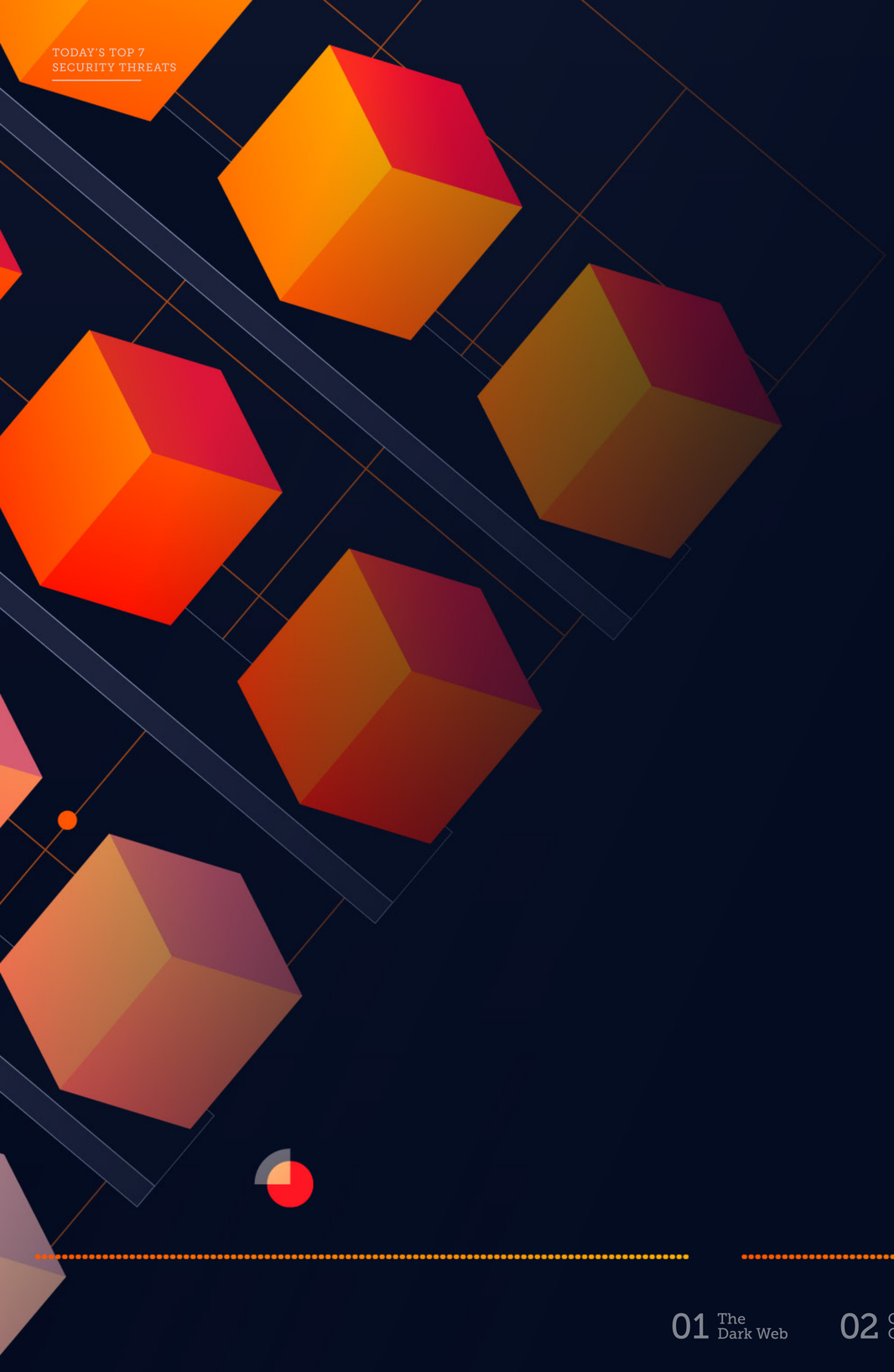
With the HP Indigo security and brand protection portfolio, you can empower multiple stakeholders, including consumers, distributors, authorities and professionals, to verify product authenticity. Use variable data and serialization to make every single package different. Then add dozens of layered security features in varied combinations with a uniquely flexible and productive on-press process, for a stronger defense and more complete control.

Gray Market Diversion>

Everyone loves a deal. Except perhaps brands, when it's their products being discounted illegally through the dubious practice of gray market diversion. Gray market diversion costs manufacturers billions of dollars each year, with a brand's actual products being sold at a far lower price than typically demanded in the local market. So, how does that happen?

Most international companies sell their products at different price-points, depending on the local market's ability to pay. This is what's called dynamic pricing. For example, the same pair of jeans will likely be sold for less in a developing country than in the US or UK. The same goes for all sorts of products from electronics to high-end purses, even diapers and toothpaste!





A scheming business person can take advantage, purchasing large quantities of products in a cheaper market (often at retail price) and diverting them for sale in another region. Thanks to the steep price discrepancy, the seller can now offer the authentic product to a higher paying public, while profiting from the difference – all without the manufacturer's consent.

Gray market diversion can also occur on an internal level, with legitimate channels or distributors redirecting inventory for sale online, pocketing the difference in removing the middleman.

Poorly managed supply chains can also play a part in the problem. Weak sales and over-saturation in one country, paired with an under-supply and the resulting shortage in another, could create a situation ripe for gray market brokers to swoop in.

There's more than just lost revenues at stake. Obtained through fraudulent means, these goods lack proper quality control. Clothes may be badly sewn, electronics improperly constructed, and perishables can potentially be put on the market after their expiration date. What's more, these illicit measures create unfair competition for the manufacturer itself, as well as authorized retailers, and over time, they could devastatingly devalue a brand.

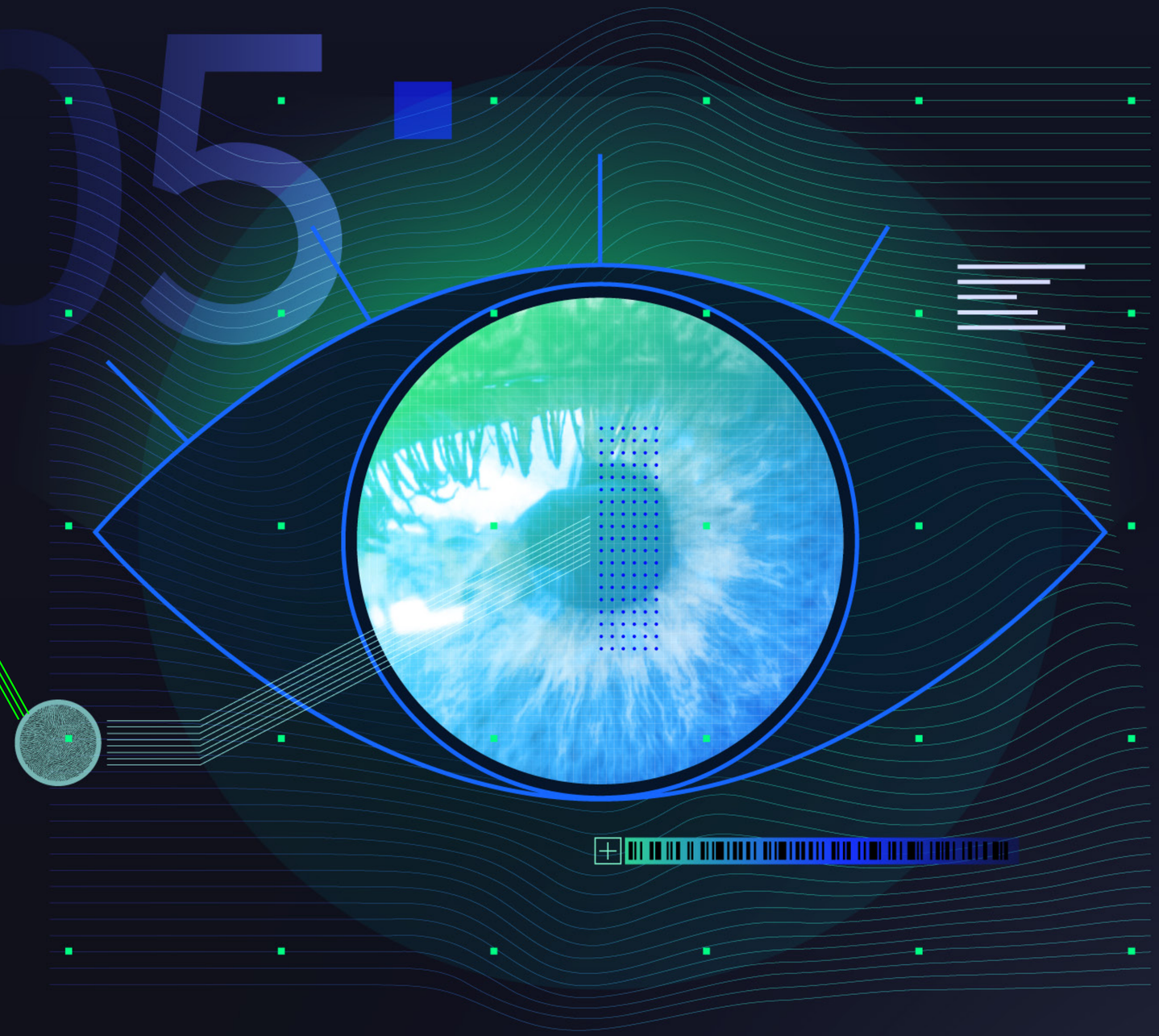
Keep Products On-Track

Adding multiple consumer authentication layers helps identify supply chain leaks and put an end to gray market diversion at every level. Using HP Indigo track & trace solutions you can embed layered designs and graphics into packaged goods. This ensures products cannot be intercepted, bypassed or sabotaged by malicious parties, anywhere, at any point.

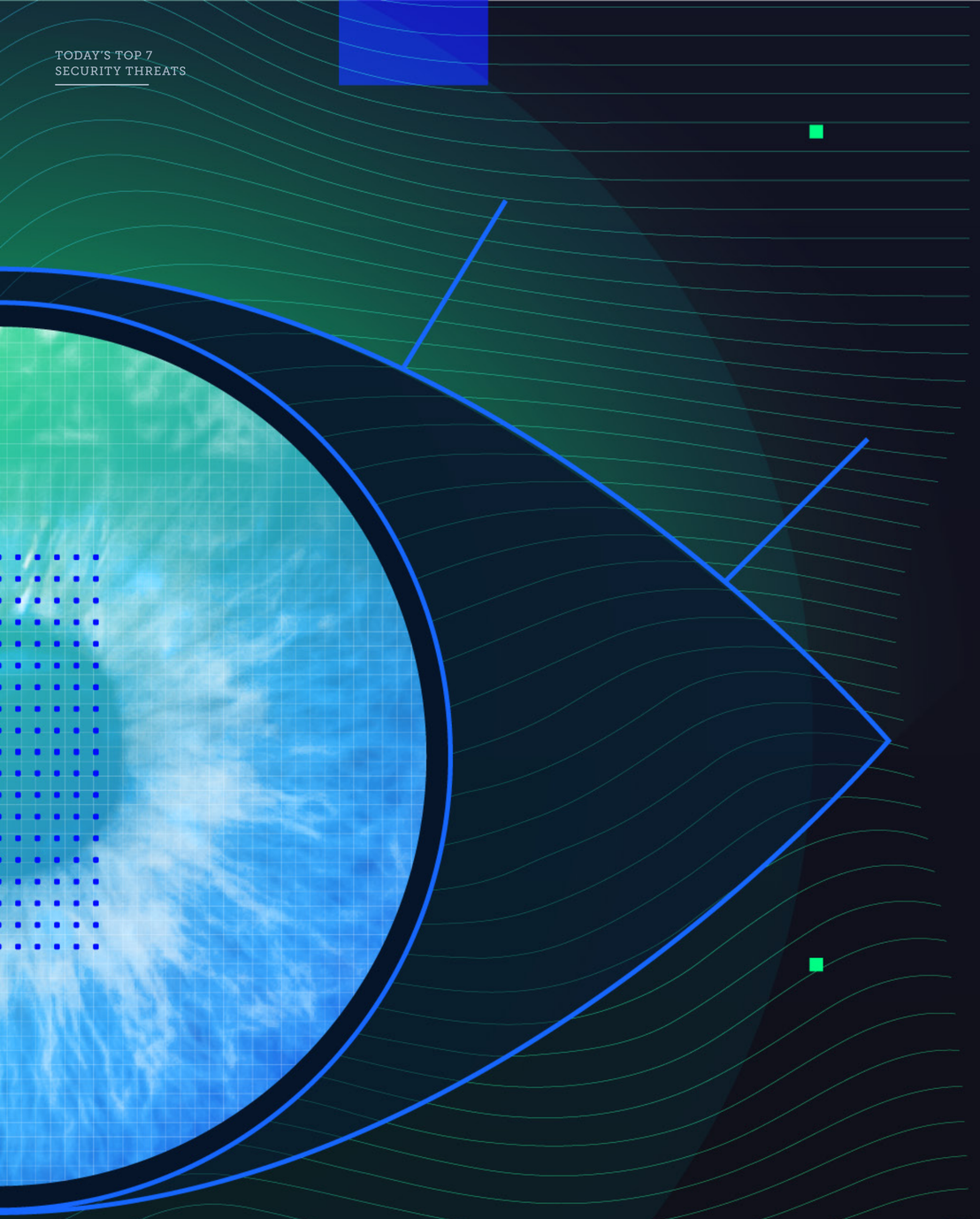
05

Identity Theft>

Keeping your possessions safe from theft is worrying enough. But now it's also your very identity you need to protect.



Identity theft affects millions of people each year; and it comes in different forms, covering a range of activities all powered by using your personal information without your permission. The most easily imagined situation is credit card fraud. But there are also plenty of instances in which people have their social security number, driver's license, or even Facebook account stolen or hacked.

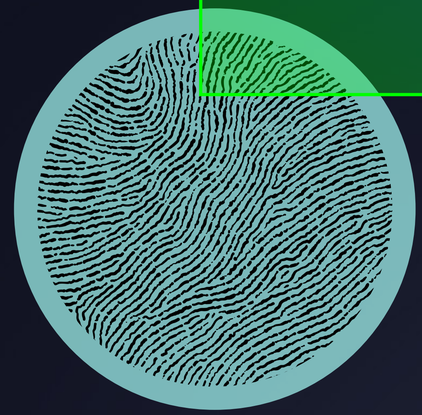


The consequences, of course, can be huge. For starters, this is a massive invasion of privacy and personal space, which can rightfully cause severe emotional distress. Then there's the financial side. While credit card charges can often be reimbursed, identity theft can damage your credit rating, payments, and even induce tax penalties along the way. Add to that the time and effort required to restore the damage, and the costs of identity theft increase significantly.

It's not only individuals who can have their identities stolen. Businesses can too. For example, on social media, competitors and haters alike can create a fake profile of a company or brand, using its name in unwanted ways. They can spread disinformation, build hostility, create forgeries, and even sell products that don't legitimately exist – inflicting serious damage on the company's image, reputation, and revenues.

Secure Identity

HP Indigo leverages versatile brand protection solutions already proven in varied industries to preserve authenticity throughout the product's lifecycle. You can use these solutions to create unique, serialized identification for product validation, as well as end-to-end cloud-based supply chain tracking.



06

Activist Attacks>

Consumer advocates can be a powerful force in promoting and protecting the welfare of the buying public. But when they take on an issue, beware.

The boycotts, letter-writing campaigns and even lawsuits these activists may bring are made even more visible through the quick spread of social media. The automobile industry, tobacco business and fast food chains certainly know what it's like – expensive, image-damaging, and potentially detrimental to the business itself. And today, just about any company or product is fair game.

While consumer advocacy cannot, and should not be stopped, it's important for brands to have a strategy in place to pre-empt the potential wrath of activist attacks. For starters, they need to know their products' potential weaknesses in advance, with answers to uncomfortable questions. Even better, the answers should be out there in the public eye, easily accessed by anyone who wants to know – long before the "attack" has begun and disinformation has spread. Food brands, for example, should make information about their ingredients and processes easy to find online. Clothing companies could easily do the same, including information on their employment practices and sourcing. And pharmaceutical companies, in addition to highlighting their extensive R&D, may want to discuss how they're able to prevent tampering. Transparency, in other words, is the ideal first line of defense.

Engagement is also crucial. Communicating with consumers through advertising and packaging is only one part of it. Social media and responsive customer support are another. Engaging with consumers gives brands an upper-hand. It shows the human face of the company and helps build trust. The better a brand's relationship with its customers, the harder it is for activists to launch an attack.

Put Up A Good Defense

While brands need protection, it's also important to let consumers police products. HP Indigo's overt layered authentication methods – such as watermarks, microtext or QR codes - let consumers see for themselves what's real, and what's not.

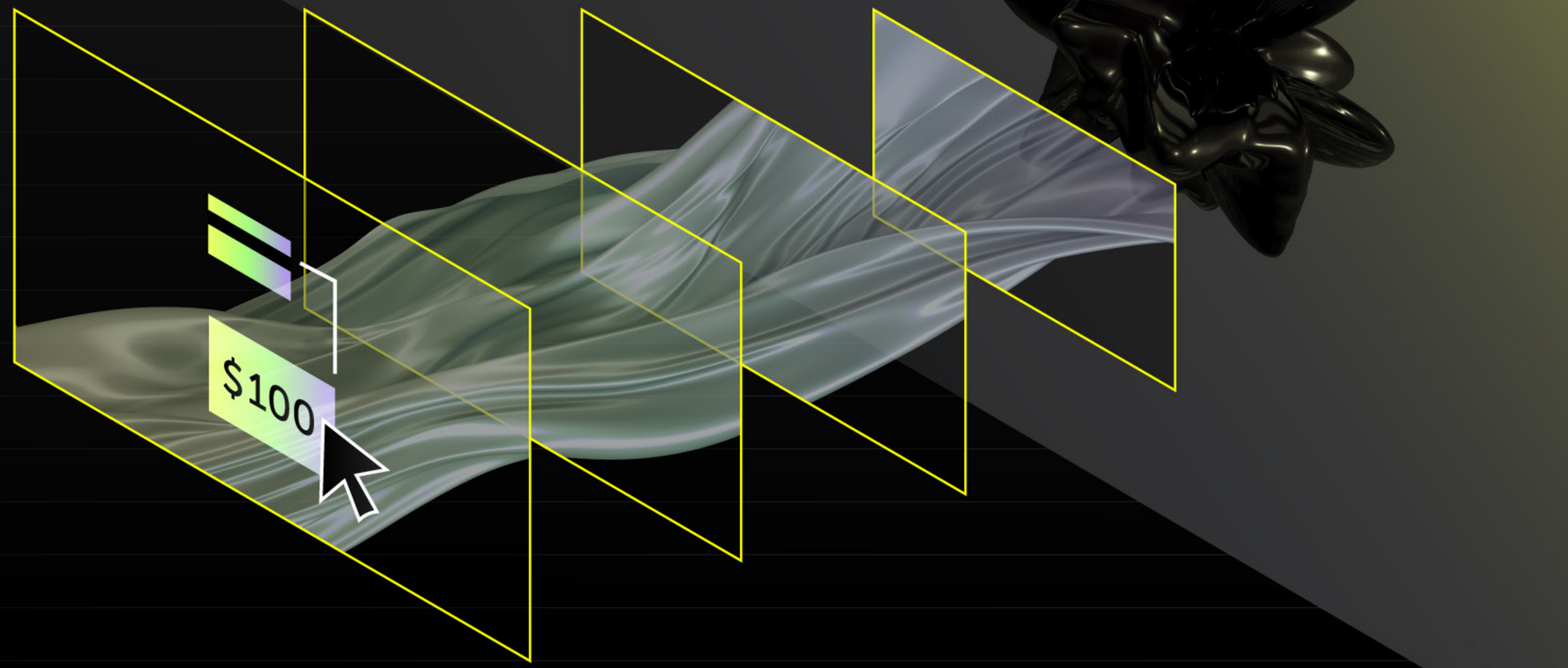
07

The E-Commerce Effect>

E-commerce is a booming business, and not just in a dollars and cents kind of way.

Nowadays, anyone can buy and sell just about any goods or service online. In many ways, it's a great democratizer, allowing everyone with internet access to engage in trade.

At the same time, e-commerce is also a facilitator of pretty much all the digital threats out there – a place where counterfeiting, piracy, gray market diversion, brand attacks, and identity theft can take place. Any site operator can add an eBay certified claim or an Amazon logo. But how well are these powerhouses out there patrolling cyberspace themselves? Likewise, anyone can say they are selling "real" brand-name products online.



Of course, e-commerce is not all bad. In fact, in most experiences it's very good. But it takes some vigilance – and ownership over the issue – to keep people and products safe.

For manufacturers, there are new difficulties to navigate in terms of pricing control, quality control, and even customer service and return policies. It's hard for them to keep track of where their products have gone and to get a grasp on their end-customer base. Consumers for their part face a sea of uncertainty when it comes to the legitimacy of their purchases, and fear falling victim to any number of scams.

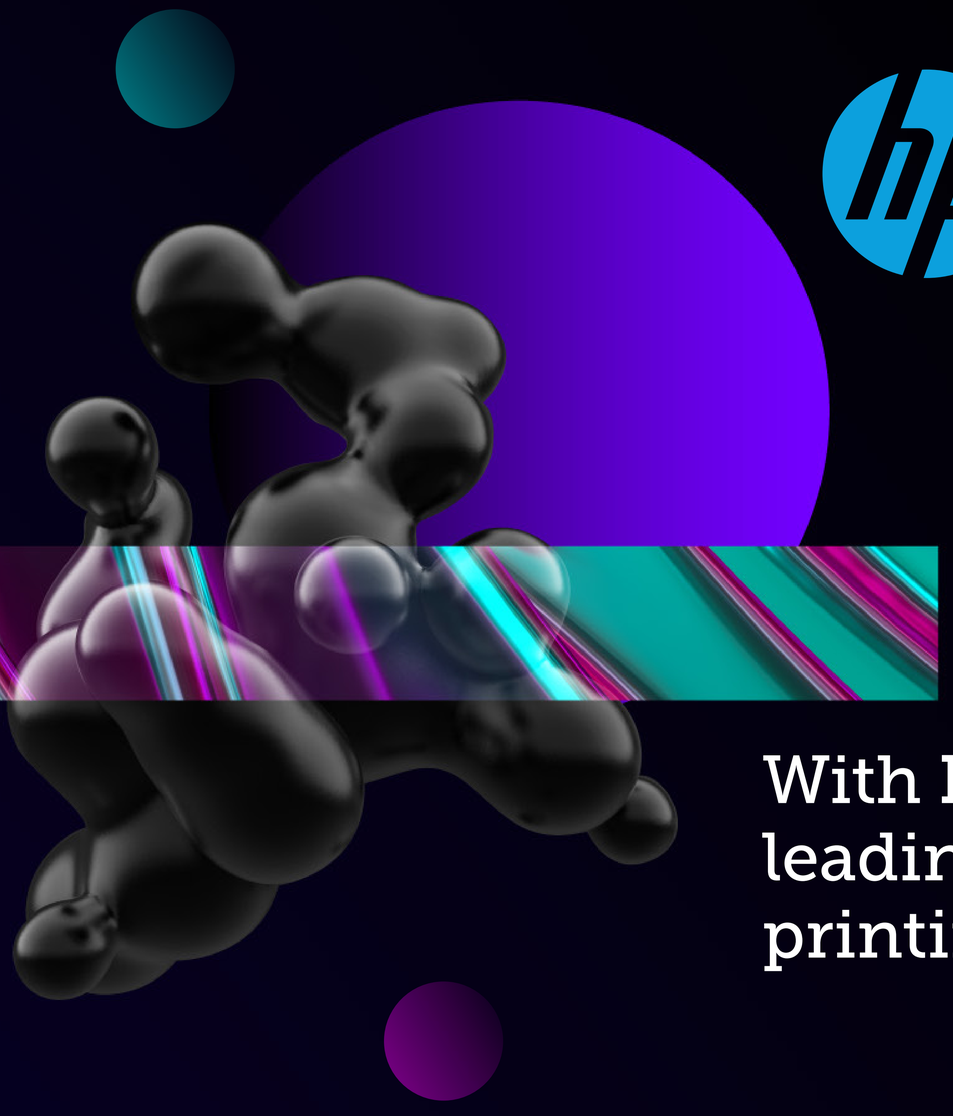
To combat the risks of e-commerce and regain control, new measures are needed to monitor and safeguard the entire supply chain. With precautions in place to protect authenticity, both manufacturers and consumers win.

Control What's Yours

Leveraging unique IDs and authentication methods from HP Indigo, it's possible to protect any product from being bypassed, intercepted, and sabotaged in any way, even in the uncertain supply chain of e-commerce. For extra security, you can add a track & trace system to identify supply chain leaks and diversion spots. Various consumer authentication methods can also be added, to reassure customers that products purchased online are the real deal.

Design by Storytellers | 4AA7-4145EEW

Get ahead of the threats



With **HP Indigo's** leading digital printing solutions

Created by HP Graphics WW Marketing, based on industry research and internal documentation.