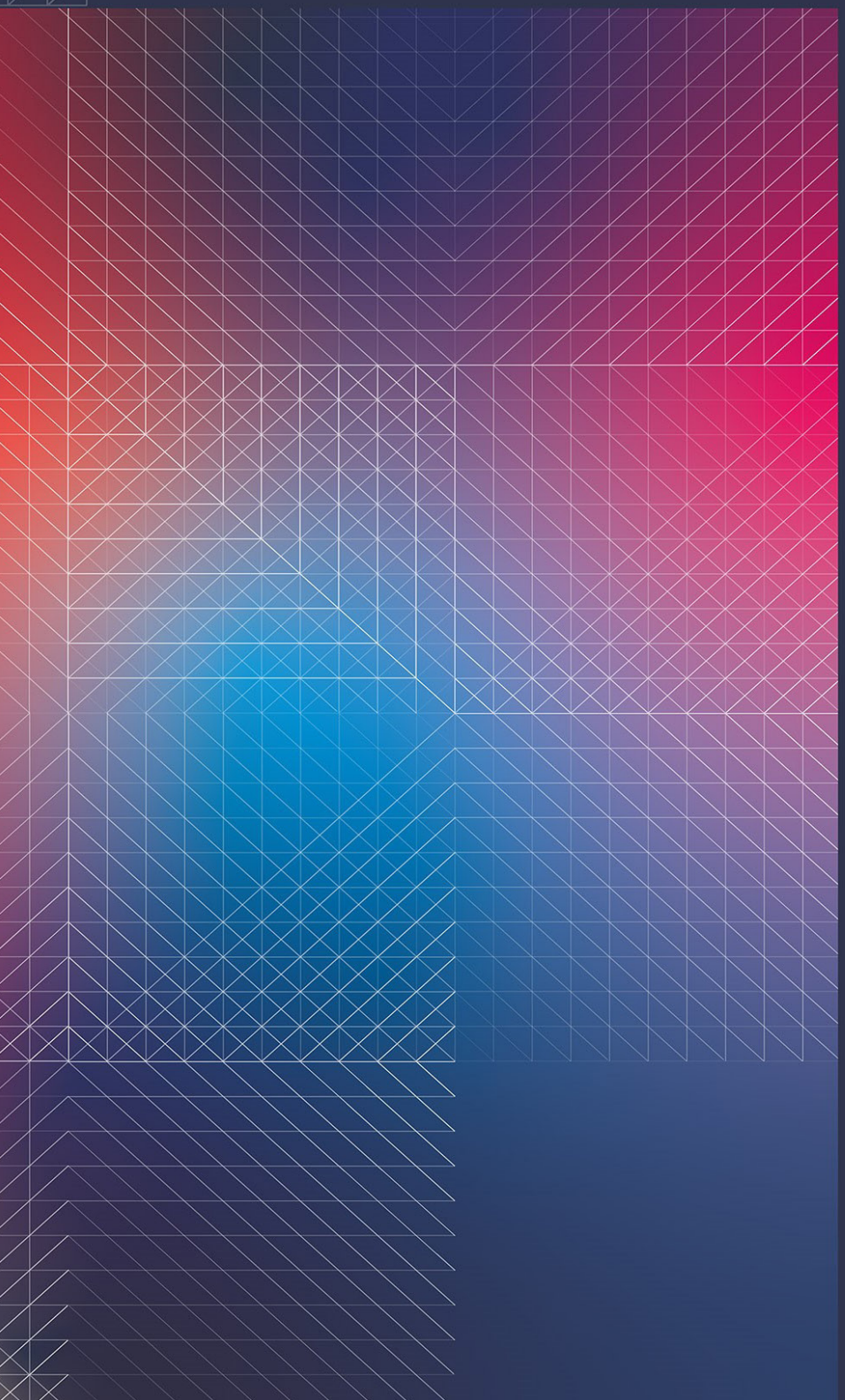
Brand Protection Insights from Industry Leaders in Gray Market, Counterfeit and IP Fraud Mitigation

December 2020



DeLaRue

Sherri Erickson
De La Rue
Key Account Director

Sherri.Erickson@DeLaRue.com
www.DeLaRue.com

FiveBy

John Solheim
FiveBy Solutions
Principal Consultant

johnsol@fiveby.com
www.FiveBy.com

Co-Sponsored by:

AGMA GLOBAL
Advancing Intellectual Property Protection

Contents

Contents continued

Report research objectives, sponsorship, and approach

Counterfeiters and fraudsters are adapting their techniques and taking advantage of the massive changes occurring around the world, bad actors are doing so with increasing sophistication and relentless energy.

The rapid growth of eCommerce in the last few years has provided a large conduit for counterfeit, warranty, and financial fraud. The Organization for Economic Cooperation and Development (OECD) detailed a 254% increase in counterfeits traded internationally — from $200 billion in 2005 to $509 billion in 2016 . At the confluence of all these changes are the issues of mitigating counterfeit, reducing channel gray market, and preventing various fraud. Brand protection programs, and the solutions designed to support them, are impacted in ways they never imagined, and manufacturers and software companies need to be prepared to address new threats.

Research objectives

De La Rue is an industry leader in product authentication with 200-plus years' experience safeguarding revenue and reputations against counterfeit and illicit trade.

De La Rue saw the opportunity to conduct first-party research to identify emerging trends in brand protection as it relates to counterfeit, fraud, gray market risk and prevention, and supply chain security.

The objective was to better understand what the industry and its leaders saw as opportunities, gaps, and unmet needs, and where brands may be exposed to greater risk and hidden costs.
The insights we sought include how industry leaders make use of, and intend to use, such techniques as security labels and related physical and digital solutions and technologies across their brand protection activities.

Sponsorship and approach

As a member in the **Alliance for Gray Market and Counterfeit Abatement** (AGMA) roster, De La Rue saw the chance to partner with AGMA and its industry global leader members to facilitate a collective effort to help unravel the pervasive and ever-evolving challenges of counterfeit and illicit trade.

De La Rue engaged an independent third-party consultant, FiveBy Solutions, to conduct qualitative research. Through co-sponsorship of this industry study, AGMA provided FiveBy Solutions with access to its members, who represent some of the largest and most influential brands in the world. Participants in the study included Cisco, De La Rue, Hewlett Packard, Hewlett Packard Enterprise, IBM, Juniper, Microsoft, Tech Data, and Texas Instruments.

FiveBy consultants conducted in-depth interviews with twenty industry leaders representing these influential AGMA member companies that operate in various regions around the world.
Results have been anonymized and aggregated to provide an industry-level view of the findings.

Details on the approach are provided under Research Methodology on page 25.

Global influences

Industry trends

Legacy

Executive Summary

Several key themes emerged from the AGMA community as predominant concerns and areas of focus for brand protection leaders. These include capabilities of counterfeiters, the impact of the pandemic, and geopolitical topics such as GDPR (General Data Protection Rights) and the impact of trade sanctions and conflicts. Besides the pandemic, these areas have been topics of community conversations for several years with mixed success on implementing tools and methodologies to address them.

Counterfeiters are demonstrating advanced skillsets and agility as evidenced by their rapid response to the landscape. In many cases, mitigation efforts such as physical security and visual identification are being effectively simulated in a few months. Financial fraud criminals and counterfeiters are using the Dark Web to communicate and exploit gaps in supply chain security measures taken by brands.

Universally, the industry leaders are looking at big data and analytics to better inform their strategies. The community is already gaining insights from such analysis, where they are better able to identify trends, understand where there are pockets of illicit activity, and quantify the scale and impact of various types of nefarious behaviors. Nearly all participants expressed an interest in more investments in analytical tools and resources as budget priorities.

Qualitative in nature and structure, the study also yielded a set of insights and trends which FiveBy sees as opportunities for deeper investigations. These trending topics had a wide spectrum of responses as to levels of preparedness to tackle, ranging from no awareness to very aware and with action plans in place.

FiveBy Solutions is a specialized risk intelligence services firm. The team brings insights that organizations need to move faster and further with the confidence to transform risks into opportunity. For over a decade, the world's most recognizable brands have turned to FiveBy when the threat of fraud, abuse, or sanctions risk more than business disruption.

De La Rue has domain expertise in high-security technologies such as holography, security print, and track, trace, and verification software. We understand how businesses operate in a complex global marketplace with multifaceted supply and distribution chains and are committed to ensuring our authentication solutions protect revenues and reputations and deliver tangible results.

De La Rue also understands that it is a dynamic marketplace. These discussions indicate more research is merited to further explore implications to interested organizations.

These include:

- Corporate Responsibility
- IoT (Internet of Things)
- Refurbished Devices
- Right to Repair Legislation

Responses have been aggregated and anonymized. The resulting synthesis leads FiveBy to suggest three potential scenarios where they have posed conceptual approaches to address some of the common challenges revealed from the study.

These could also merit further exploration, and include:

- Third-party Data Management Platform (DMP)
- Component Inventory
- Third-party Rating System

Global influences affecting brand protection programs

Industry leaders across the AGMA community noted a handful of global issues that are influencing brand protection in unprecedented ways.

- **Acceleration of counterfeit.**
  Counterfeiters and fraudsters are expanding into new markets while in parallel they continue to advance their capabilities as fast or faster than brands can address them through current programs and technologies.

- **Expansion of market vulnerabilities.**
  COVID-19 has introduced both direct and indirect impacts on the way the global market purchases and sells goods, and the scale at which counterfeit and illicit trade is propagated.

- **Complication of trade.**
  Both GDPR and geopolitical issues involving trade conflict are contributing to increased complexity and more obstacles to the distribution of legitimate products into certain regions, and at the same time limiting investigation capabilities and global brand protection program effectiveness.

> "I think technology and maybe the counterfeit space is much more sophisticated than it maybe was 20 years ago. I think it's probably a lot easier too for counterfeiters to print acceptable, passable, simulations of secure print vended products.
>
> **~ Study Participant**

Independently, each global issue creates an added level of complexity to thwarting counterfeit and illicit trade. Collectively, they represent the potential need to rethink and re-engineer brand protection programs altogether.

Acceleration of counterfeit

The study highlighted how counterfeiters today are savvier and more adept at adapting to, navigating around, and taking advantage of changes in the market.
Participants noted these fraudsters are more sophisticated, with greater technical resources, and they can consistently produce credible counterfeit security labels in less than six months from the time the legitimate product hits the market. Digital transformation is proving to be an accelerator of illicit activity. Counterfeiters have broader access to a larger portfolio of digital data for harvesting and exploitation. The Dark Web, and other similar forums supporting the distribution of intelligence on unlawful activities, facilitate information sharing amongst bad actors.

Arguably, fraudsters may be more advanced in communications, based on their collective effectiveness in exploiting gaps in security. Legitimate brands tend to share information with each other on a limited basis, which could contribute to common gaps for counterfeiters to attack multiple organizations for prolonged periods.

> “
>
> Fraudsters are savvier, sharing information amongst each other, producing counterfeit at an accelerated pace, with increasing scope and scale, and brand protection programs are challenged to stay ahead.
>
> **~ Study Participant**

The scope of counterfeit is expanding. Products that may not have been interesting to counterfeiters in the past could suddenly be in the crosshairs of their attention, as has been seen with COVID-19 healthcare products and the unprecedented proliferation of counterfeit masks, test kits and sanitizer.

Expansion of market vulnerabilities.

Experts agreed that the COVID-19 pandemic has changed the way goods are sold and purchased around the world, but less understood is its impact on product distribution, authentication, and investigations. Implementing remote capabilities has challenges across resources, technology, investment priorities, and effectiveness.

Another concern is the growing risk of diminished brand integrity because of illicit activity increasing in both scope and scale. The acceleration of counterfeit is further enabled by the increase in online commerce. Brands that used to rely on their own distribution partners to sell their products may now find themselves relying exclusively on online channels where they have less visibility and control.

Consumers and businesses are facing economic pressures, they are looking for better deals, and they are having to rely on the internet where online scams are proliferating. Product authentication is proving to be challenging in an online world and this opens broad opportunities for fraudsters to profit.

Industry leaders are universally aligned in their expectations that the impacts of the pandemic will endure for the foreseeable future and this is forcing brands to reassess their priorities and budget allocations.

> “
>
> COVID has thrown a wrench in a lot of things - in that we are reassessing budgets and what is necessary, based on the current knowledge we have today.
>
> **~ Study Participant**

Complication of Trade and Trade Sanctions

Two geopolitical issues were highlighted as having major global impacts on the distribution of legitimate goods and a brand's ability to protect their revenue. These concerns are centered around trading laws and the EU's General Data Protection Regulation (GDPR).

Trade restrictions are not a new challenge and have long contributed as an enabler of new channels for illegitimate commerce. Restrictions stemming from major markets like the United States, the European Union, and China, among others, stifle legitimate trade. Trade conflict can result in borders being closed, tariffs becoming punitive, customs agents being decommissioned, or other barriers imposed. Fines for not having good visibility and risk intelligence of your import and export parties are going up.
The pandemic has exacerbated the cross-border trade challenges and created more opportunity for fraudsters.

RISK ASSESSMENT

Industry leaders in brand protection are concerned that geopolitical issues such as trade conflict and GDPR are making it more difficult for brands to distribute legitimate product, thwart illicit trade, protect revenues and reputations, and enforce their IP.

Demand for the industry's products has not diminished and if customers are not able to purchase authenticated product when they need it, they are more likely to be the victim of counterfeit or grey market. Brands recognized that this is an issue beyond their control, but it's one that has a direct and growing impact on their business and it challenges both their ability to ensure customers get the genuine product they expect and believe they're paying for, and their ability to enforce against illicit trade.

GDPR is relatively new on the international scene, having become enforceable in May 2018. Whilst there is some flexibility within the regulation to be adjusted by individual member EU states, it is directly biding and applicable. GDPR has been broadly adopted as the global standard for personal data privacy. The study revealed that GDPR is creating complex challenges for their global brand protection programs. Flexibility within the regulation has led to copious and complex regional variations that prevent brands from rolling out programs in a single, global format, as was possible under previous regulatory guidelines.

Enforcement and preventative measures were noted by industry subject matter experts to now be more expensive and less effective because of GDPR implementation. Economies of scale are no longer sustainable and brand protection budgets struggle to meet their needs.
Some brands expressed interest in implementing an "all-digital" model for their prevention and detection solutions, where they would decrease their dependency on physical authentication mechanisms in favor of fully digital verification. GDPR inhibits achieving an all-digital goal by introducing more restrictive limits on digital tracking in certain geographies.

Industry trends impacting the approach to brand protection

Brand protection leaders together identified four trends they expect to have an impact on the industry at large, their organizations to varying degrees, and their roles, either directly or indirectly. These include corporate responsibility initiatives, the Internet of Things (IoT), refurbished devices, and right to repair legislation.

Corporate Responsibility Initiatives

Universally, brands agreed that their organizations broadly support and are focused on attaining sustainability, carbon neutral goals, and fair-trade practices, and they are beginning to push these requirements out to their supply chains. Most brands have well-established programs in place, and they are seeing an emerging interest in using end-to-end product tracking technologies to measure the company's carbon footprint.

SUPPLY CHAIN

Track & Trace is the system for production data capture and product association inside brand manufacturing facilities, that records the usage of secure labels and their affixation to products. Products are then tracked through packaging and shipping.

Brand protection leaders have a unique set of tools and expertise in their arsenal to help their organization assess its environmental impact. Track and trace technologies are widely utilized in authentication solutions to verify a product is legitimate throughout the supply chain to end users.

Sometimes referred to as physical-to-digital solutions, this is typically done by associating a serialized token such as a holographic label with a data tracking system used by the brand as anti-counterfeit and anti-diversion services. The data capture systems could be adapted to encompass a broader product data set associated with other product components and simultaneously deliver more robust carbon footprint data. These existing technologies offer a potentially cost-effective and efficient way for an organization to leverage brand protection expertise to support a companywide carbon neutral goal.

Arguably, counterfeit product is more likely to contain substandard materials that could be more environmentally hazardous, so a side benefit of securing the supply chain through robust track & trace solutions would be the further assurance of carbon neutral efforts under the brand's control. Study participants noted that corporate responsibility initiatives are typically owned by groups outside brand protection and this could represent a barrier to integration. They generally agreed that their expertise in track & trace and the system's ability to append and aggregate data could be expanded to include carbon footprint.

Internet of Things (IoT)

IoT is the interconnection, via the internet, of interrelated computing devices provided with unique identifiers, embedded in everyday objects, enabling them to send and receive data, without requiring human interaction.

Interconnectivity among multiple devices brings convenience to the consumer market and efficiency and intelligence to commercial enterprise organizations. For brand protection experts, IoT introduces complexity, a multitude of unknowns, and no clear answers.

Device producers are concerned about waste and its commensurate impact on the environment. Manufacturers have seen how IoT technologies offer them opportunities to reduce waste by extending the useful life of products through field monitoring and signals generated when a component needs changing instead of having to scrap the entire product.

Benefits such as waste reduction may enjoy broad support across an organization, but they may be offset by the often-indeterminate number of vulnerabilities that IoT introduces. Top of mind for brand protection leaders is a broader and potentially uncontrolled landscape for bad actors to exploit systems, access data, introduce malware, and disrupt business.

A brand may have to weigh the benefits of interoperability against the risks of not having controlled or "locked" proprietary systems. This balance may shift as more and more devices and their interior components communicate and share data, with increased frequency and at greater scale.

> IoT presents challenges and opportunities for brand protection leaders to thwart bad actors before they take advantage of vulnerabilities by introducing malware, exploiting systems, accessing data and disrupting business.

Participants broadly agreed that IoT is likely to have a high impact on their business, but none were able to provide a clear assessment of how it will affect their business, or product roadmaps, or what they, as brand protection owners, should incorporate into their strategies to address the vulnerabilities presented through IoT proliferation.

Refurbished Devices

Refurbished devices have been a part of most device manufacturers' portfolios for decades, and leaders in the industry categorically agree that this channel has historically been at high risk for fraud, the introduction of counterfeit, and security-compromised technology.

They also unanimously agreed that these known risks are likely to grow, even exponentially. New life has been instilled in this older channel through several factors in the market today:

- Economic pressures with consumers and businesses seeking better deals
- COVID-19 related spikes in demand due to work-from-home, study-from home
- Environmentally minded workforce raised with the mantra to “reduce, reuse, recycle”

Many brands, including device manufacturers and software vendors, created a new distribution channel when refurbished devices became a network for growth. They established programs to authorize and manage the channel, expanded mechanisms for line of site over legitimate use of their product, and some even offered incentives to become a certified partner.

Refurbished Devices are a channel known to be at high risk for fraud, counterfeit and security compromised technology, Industry leaders see the potential for high growth in this channel and the increasing need for brand protection programs and physical-to-digital authentication solutions to address this growth trend.

Brands with authorized or certified Refurbisher channel programs are providing these partners with product authentication solutions that provide assurances to the end customer that the product they’re buying is genuine. Adding track and trace digital capabilities to a secure physical token, such as a holographic label, provides brands with greater line of site into the refurbisher channel and as their devices are distributed in the market.

The refurbisher participating in these programs gains the trust of the end customer and positions themselves for future growth and brand integrity. As the industry is aware, the bad actors tend not to join these programs and that is where the challenges largely lie.

Where the refurbished channel is unmanaged and uncontrolled, there is an increased risk to brand reputation. The end customer purchasing a refurbished device does not distinguish from the brand’s promise, expecting it to function as a fully authenticate device with genuine, secure components and not one that might be compromised with counterfeit or inferior parts. In this scenario, the brand’s reputation suffers, not the refurbisher’s image.

If the customer is expecting warranty coverage for a refurbished device that contains non-genuine components, or if the Refurbisher is submitting a warranty claim for a device that has been compromised with counterfeit, the item may be subject to warranty fraud.

Right to Repair

The study revealed that while device manufacturers are increasingly concerned with pending legislation that could impact how they and their customers prefer to manage device repairs, most brands do not yet have plans or solutions in place to address it when it comes into law. For many complex or high-tech products, vendors have made it difficult to get the repair parts, tools, or physical access to the components to repair devices outside of official channels. US laws have been proposed to support right to repair, and the European Commission has the aim is to embed a "right to repair" in the EU consumer and product policies by 2021.

Right to Repair legislation originally came to life as an environmental effort to reduce waste.
It has evolved in recent years to encompass policies that make it easier for consumers to choose the who, what, when, where, and how much they pay for repairing a device they buy.

The legislation could also include measures requiring manufacturers to make products and components more accessible to repair. Many brands prefer to maintain control over device repair, through their own or authorized repair partners, to ensure consumer safety, device performance, integrity of product design, and component authentication. Brand protection experts see significant challenges for brand owners should the legislation be more broadly enacted. Legislation is already in place across Europe and in some US states, and the consumer-focused policy is engendering broad support.

Top of mind are risks for increased warranty fraud and the potential for introduction of low quality, counterfeit, or security-compromised components. The types of risks are like what the Refurbisher channel introduces, but in the case of Right to Repair, the risk landscape could open to a much broader, unmanaged group of repair shops, thereby increasing the scope and scale of the issues.

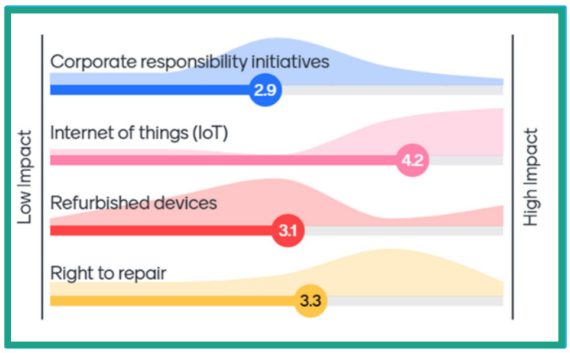
Brands need a way to verify and certify that only genuine components are used when their devices are repaired. They will need to support warranty claims, product performance expectations and customer satisfaction, product liability concerns, and brand reputation.
As with the Refurbisher market, a physical-to-digital authentication solution can provide device manufacturers with a mechanism to connect genuine components to verifiable devices and create a record of provenance.

In some instances, the brand protection teams are not connected with the manufacturing or operations teams who typically support these claims, so it is challenging to bring solutions to the business.
This disconnect is highlighted among the legacy challenges that will be discussed in the next section.

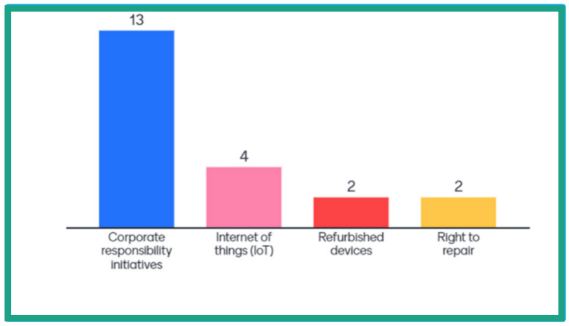
Barometer of Findings

During the AGMA Americas Virtual Conference on August 19th-20th, 2020, attendees were invited to participate in a few quick surveys in an interest to gauge whether the above insights were relevant to what attendees were also experiencing.

Audience members were asked to rank the importance to their business of the above Industry Trends as to having a likely high or low impact, with a sliding scale of 1-5 with 5 being the highest. Results below show that IoT had an average 4.2, followed by right to repair at 3.3 and refurbished devices at 3.1.



When asked the follow-on question inquiring which of these trends, they have a plan to address, it became clear that they are least prepared for those that would be the most impactful to their business.



Legacy challenges among leaders in the industry

The leaders surveyed for the study represent not only some of the most influential brands in the industry, but they also individually and collectively represent a vast breadth and depth of knowledge pertaining to counterfeit, grey market, fraud, and supply chain security. Their expertise spans decades of knowledge and their individual tenures in the brand protection arena range from seven to more than 20 years.

Much of what the study focused on was forward looking, on emerging trends, but it also revealed that in some regards, they have inherited a myriad of obstacles that are difficult to overcome. Four challenges emerged as common themes shared among the group: customer engagement, component verification, supply chain, and business group misalignment, the most prominent being the latter two.

Customer Engagement

Consumers are barraged with offers across various marketing channels, under pressure to secure the best deal, and overwhelmed with the amount of information available to evaluate to make purchasing decisions. Their motivation, and the effort it takes, to determine if a product is the genuine article has wallowed in their indifference for years, and brands have been battling "counterfeit apathy" among all the other challenges they face. Brands invest in numerous techniques to thwart fraudsters. The effectiveness of overt and covert technologies is diminished by the customer's unwillingness to take advantage of the measures available to protect themselves from unscrupulous actors. Finding new ways to engage customers was noted as challenging, with some attempts seeing temporary success, other endeavors having potential not yet realized, a few mechanisms seeming to have promise, and they're continually needing to find a balance between risk and reward. No silver bullet emerged as a best practice solution.

Various approaches have been tried, including:

- Customer enticements and incentives to authenticate
- Consumer warnings that warranty coverage could be voided and at risk of fraud
- Requiring customer acknowledged actions to activate the product, such as through the correlation of embedded activation sequencing with license key entries
- Mobile phone-based authentication apps
- Incorporating overt brand authentication with the digital user experience

Brands are concerned that whatever method they employ to engage, enhance, and enforce their IP, it does not detract from the overall customer experience. This is proving to be a long-standing and moving target.

Component Verification

Industry trends such as refurbished devices and right to repair legislation are putting a spotlight on the enduring challenge to verify the authenticity of components within a device.

Most brands have downstream distribution channels, and some are more complex than others. A genuine product is packaged and shipped, aggregated into distribution, disaggregated across resellers, reaggregated into retail, disaggregated to consumers, reaggregated through returns or repair channels, and so on.

Tracking the device itself is a challenge and having to track the components within that device adds a layer of complexity that can be daunting. For some brands, this is a much bigger problem than having an entire device counterfeited. Fraudsters are purchasing genuine product, disassembling it, and embedding genuine parts into otherwise counterfeit, or alternatively, introducing counterfeit components into an otherwise genuine device.

> “You need the ability to show customers the bigger picture of what you are doing as a company to protect their purchase.
>
> **~ Research participant**

For one brand, this is the cornerstone of their counterfeit attacks. Each node in the channel can track provenance of data within their remit of distribution. However, unless it is mandated by contractual terms, the data is not usually shared back to the brand. Even if component level data was available, it would require the distribution channel to share the data.

Another underlying legacy challenge is one of trust between brands and their channel partners, and a lack of trust leads to gaps in what is shared, if not barriers that result in no data sharing at all.

Some brands do not trust partners to conduct thorough due diligence, friction exists over who owns the customer relationship, and partners are wary that brands will steal “their” customers if data is shared.

The study revealed that these leaders are looking to emerging technologies to help gain end-to-end visibility, and greater control, of product and component movement. Noted were IoT, advanced data analytics, and Blockchain, which are covered in the Technology Trends section of this report.

Supply Chain

The supply chain feeding into most brand's brand protection programs is typically complex and interdependent. Brands have invested heavily in infrastructure development to meet exacting requirements to thwart counterfeiters who have targeted their brand. This includes vetting and onboarding third-party partners, logistics, operations, security, and more, and costs have been in the multiple millions of dollars to establish a high-functioning supply chain.

This sometimes results in an entrenched supply chain and the challenge this creates for brands is having a mechanism for agile adoption of new technologies and countermeasures to address rapidly evolving counterfeit attack vectors.

Making changes to the supply chain, whether broadly or with a single vendor, faces strong resistance in some organizations due to the direct and indirect costs involved. The initial investments would have to be replicated and amplified to modify supply chain methodologies, qualifications, and stock-out mitigation strategies. If funding a change is driven only by the brand's operations or antipiracy teams, there is generally a lack of broad organizational support.

> "We need to help business owners see the problem that's coming around the corner. Because often, they are not accepting that their new product will suffer the same spears and arrows of piracy that others do.
>
> **~ Research participant**

An agile supply chain that has the capability to incorporate third-party technologies is seen to be an advantage, as are solutions built on modular platforms that can more rapidly respond to emerging counterfeit threats. Also noted to potentially have an impact on supply chain initiatives are the advent of IoT, advanced analytics, and Blockchain technologies. A report by Boston Consulting Group estimates cost savings representing 0.4%-0.8% of revenues could be attained by implementing these technologies.

Business Group Misalignment

Brand protection teams are typically situated as a standalone group within organization structures. This works for many organizations where an agnostic view of business results is desired, when there is a high risk and large counterfeit, grey market, fraud, and supply chain security challenge, and where a unified cross-company antipiracy strategy is most effective.

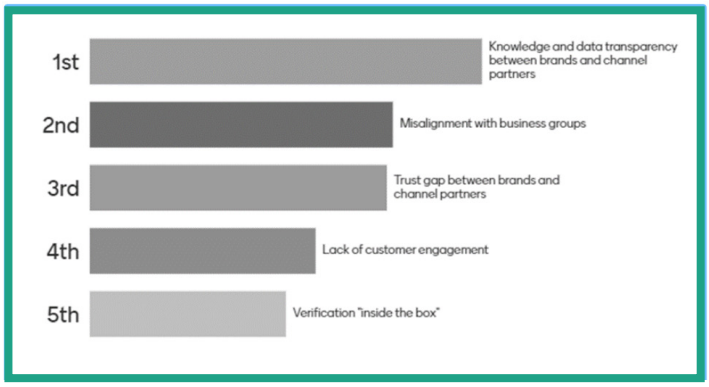
The study corroborated that the long-held challenge of organizational misalignment endures between brand protection and other groups. Only a few could point to strong collaboration and objectives alignment among their own group and sales teams, product groups, business owners, and corporate responsibility teams.

They universally agreed that this lack of integration leads mostly to lost opportunities for the company at large. Brand protection groups, with their agnostic, cross-company perspective, their charter to protect and recover revenues, and their data-driven, results-oriented methodologies, are in a unique position to help business groups forecast risk and proactively mitigate for it.

The advent of physical-to-digital solutions and the wider reaching benefits this could deliver across the company makes it more imperative than ever for these groups to collaborate.
A handful of study participants were placed in sales operations or sales enablement groups and they expressed this may contribute to being more successful at improving their impact on the wider business. Due to the qualitative nature of the study and the sample size being relatively small, it is not possible to draw any conclusions.

Validation of Findings

During the AGMA Americas Virtual Conference on August 19th-20th, 2020, attendees were invited to participate in a few quick surveys in an interest to validate whether the above insights were relevant to what attendees were also experiencing. The Legacy Challenges of the audience are ranked below in order of priority, with “Knowledge and data transparency between brands and channel partners” leading the pack.



Technology trends sparking interest from brand protection experts

Leaders across the industry are curious to learn about trends in technology that could have a positive impact on their ability to mitigate counterfeit, grey market, fraud, and supply chain security. The survey sought to uncover leading technologies that they found exciting, to discover if there’s anything new they’re doing for their business, and to gain insights into what they may have tried that worked, or didn’t work, and why.

> “A lot of people don’t really care so much about the technology itself, but what the technology will allow them to do.
>
> **~ Research participant**

The most common response among participants was that various technologies, per se, can be a valuable tool, but more important was aligning the technology’s fit with their strategy. Some technologies were agreed to show promise and are considered front runners in their evaluations for adoption; others are thought to be interesting but not ready for implementation and are being monitored for potential future consideration. This paper highlighted several technology trends deemed to be of the highest interest, including big data and analytics, automated monitoring, and removal services, blockchain, modular customization, and intra-component communication.

Big Data and Analytics

Universally, leaders were most excited about what big data, advanced analytics, machine learning and AI could do for their business. This was the area they were most interested in investing in, through adding data scientists and analytics resources, shifting from reactive to more proactive measures through data analytics, or simply having better data, more access to data, and better visibility of data across the supply and distribution chains.

> **Wish list for data:** Visibility of the level or risk, the full picture and being able to say that we know where we are. From there, you can get the budget.
>
> **~ Research participant**

Most participants expressed a similar view that there is more value in big data and analytics than is found in basic tracking technologies in the market. They were less concerned with micro-level tracking of real-time product location and more interested in macro-level analytics pertaining to bigger trends and patterns of activities that could support investigations or identify potential vulnerabilities that could then be mitigated.
The majority pointed to this area as a priority for investment.

Advanced analytics would also give these leaders the data they need to build a business case for budget and resources. It would help them illustrate the issues in a compelling, data-driven way that supports their argument for why other groups in their company ought to better align with the brand protection team.

No specific examples were given regarding how these technologies could, improve their brand protection efforts. References were made to the data potentially available at each node in the value chain that they have no access or visibility to, whether from a reluctance or inability to share data. This creates opportunities for grey market operatives and can strain the relationship between manufacturers and distributors.

These leaders highlighted the demonstrable value of being able to shift from taking reactive measures to implementing proactive actions. Their ability to do so is predicated on being better informed through intelligence and insights provided by more robust data analytics.

Better data quality, greater data access, more data analysts, and improved visibility for their efforts were agreed to be the benefits of big data solutions for brand protection problems.

Automated Monitoring and Removal Services

The acceleration in scale and scope of online transactions, largely a result of the pandemic, and the commensurate escalation of fraudulent online sellers is contributing to the need for more robust automated solutions.

Technology that enables automated monitoring of online activity and the corresponding automated removal of these bad actors was universally highlighted as a successful tool.
It was noted that average selling prices of online transactions are increasing, indicating more consumer confidence in spending larger amounts through internet purchasing exchanges.
As noted above in the discussion on expansion of market vulnerabilities, brands may also be in a position where their channels of distribution have contracted, and they now must rely more heavily in ecommerce to sell their high-priced products. These dynamics make it attractive for counterfeiters to exploit.

Blockchain

Blockchain has been discussed and evaluated for several years and it was a hot topic for debate amongst participants. All agreed that while it is a technology-of-interest, it is not yet mature or secure enough to match its potential.

Leaders saw the greatest area of opportunity for Blockchain is in its ability to track the provenance of a product and its components from supply chain through the distribution channel and throughout a circular economy. This is facilitated by Blockchain secure key algorithms.

Trends such as refurbished devices and right to repair are contributing to the opportunities for Blockchain to be a game changer. A few participants in the study, who represented mature supply chain organizations, are in the early testing phases of Blockchain usage, and others are keeping it on their radar.

Modular Customization

Modular customization is not a technology in and of itself, but it is a strategic approach to combine, layer, and interchange technologies. The overarching benefit of modular customization is in its agility, which results in an ability to rapidly respond to counterfeit threats by ripping-and-replacing technology components in a planful way. Technology layers could include a hybrid of overt and covert anti-counterfeiting features, or an interchangeable mix of digital and physical solutions.

Supply chains that are doing this successfully are also able to minimize costs and maximize efficiencies by building solution roadmaps on a modular platform.

Intra-component communication

Imagine components inside a device taking a self-inventory, validating amongst themselves whether they are all present and accounted for, and whether they are all genuine, authorized components. Or not. This illustrates the concept of intra-component communication.

Intra-component communication technologies could enable enhanced digital verification to identify, and even prevent, warranty fraud. These leaders noted that this could improve the end-customer experience. Other scenarios where this technology could apply include refurbished devices, right to repair, IoT, and supply chain security, to name a few.
An example where this technology could be amplified includes big data and advanced analytics, where brand protection teams could look at outputs from intra-component communication at a macro level.

Experts mentioned area- and near-sensory capabilities, such as RFID and NFC, as the methods most evaluated for digital verification. These technologies tend to come at a higher cost and have some limitations around use cases, and most participants did not see an immediate practical application due to unacceptable ROI.

Suggested emerging scenarios on the precipice of brand protection interests

Throughout the course of the study, FiveBy Solutions consultants were able to glean unique insights and perspectives into the challenges faced by brand protection leaders. Several themes emerged that pointed to additional opportunities for continued dialogue, further research, and problem solving.

Following are three scenarios developed by FiveBy which may represent potential solutions to several issues raised by leaders in the industry. These include third-party Data Management Platform (DMP) and analytics, component inventory, and third-party partner ratings. For each scenario, the problem statement and corresponding opportunity is identified.

Third-party Data Management platform and Analytics

Problem Statement:
Painting the big picture through data requires access from several angles to data sources. The primary challenge associated with data management is that data sits in disparate systems. There are significant gaps in the data available to brand owners due to the lack of information shared to and from channel partners, as discussed earlier. Today, data sharing requirements are contractually bound and there is a lack of trust among brands, vendors, and channel partners. To make matters more difficult, channel partners are not typically required to share data with brands unless it is tied to incentives.

Opportunity:
There is a seemingly clear opportunity to partner with a third-party DMP and data analytics company to collect and analyze trends and patterns that could be shared with brands in a way that protects proprietary intelligence. This independent, third-party data resource could potentially provide the analytics that all participants were eager to highlight as areas of investment. Potential uses are identification of logistics friction, end user consumption and activation trends, fraud hot spots, and many more potential insights.

Component Inventory

Problem Statement:
A device's internal components are generally easy to replace with lesser quality or counterfeit parts and they are often sold as a replacement for a warranty repair, resulting in the brand's all too common and costly problem of fraud. To qualify for warranty repairs and reimbursement, and to ensure consumers get the true and full experience a brand offers, these components must be authenticated as genuine.

Opportunity:
A potential opportunity is to use IoT, RFID, or NVC solutions that interact digitally with encrypted keys for user authentication. Some of these technologies may also be embedded into secure labeling for combination of visual/digital verification of genuine product.

Third-party Partner Ratings

Problem Statement:
As noted previously, a legacy of mistrust exists between brands and their channel partners. This is further magnified by a brand's global efforts to sell products directly to consumers, such as enabled by subscription-based pricing models, advanced online transaction capabilities, and automated self-support tools. According to participants, they expend considerable effort to internally rate channel partners based on the limited information they collect directly. As a result, some brands need to narrow the number of authorized distributors or pursue direct distribution model. And some less-than scrupulous partners make it through the cracks in intelligence needed for well-informed decision making.

Opportunity:
Limited information sharing and redundant efforts for most of the brands to evaluate, assess, and onboard ecosystem partners creates an opportunity to improve the efficiency and confidence in selecting channel partners. Many brands work with the same partners and the respective information sharing could benefit all brands collectively.

An objective, third-party rating system could monitor channel ecosystem performance and allow for a more efficient partner selection process. Much like a credit rating mechanism, partners would receive updates on performance and earn ratings, thereby indicating risk levels. Legitimate partners will strive to maintain and improve rating scores, while fringe partners may be more readily identified. Further, this concept will improve communications and information sharing which can narrow gaps for counterfeiters and grey market actors to exploit among brand organizations.

Summary

This study yielded a range of intriguing and sometimes unexpected insights from a cross-section of representatives from AGMA member companies. The purpose of the research was to identify and share unmet needs, today and into the future, and spotlight trends across the industry that could impact brand protection programs. Several clear consensus points emerged in this initial discovery effort.

First, the major themes encompassing advanced counterfeiter capabilities, COVID-19, and geopolitical regulations drove top of mind concerns amongst the participants. These topics are expected to become perennial challenges for member companies. The lingering impacts of the pandemic and managing through a changing regulatory landscape are emerging as more complex and posing both challenges and opportunities.

Second, a set of industry trends emerged where brands are at varying degrees of preparedness to address them. IoT, refurbished devices and right to repair legislation lead the list for likely to have the highest impact on their businesses but are least equipped to address. Whilst brand protection leaders have unique expertise and tools to aid in the development of solutions, coupled with legacy challenges these teams face, there may be a need for third party resources to facilitate their implementation.

Finally, technology as it relates to big data and the use of advanced analytics were highlighted as the top priorities for investment and desired budget allocation across all participants, regardless of organization size or brand protection program maturity. Due to disparate product types, channel models, brand protection priorities, resource constraints, and GDPR regulations, going “all digital” was acknowledged to not be viable in the near to mid-term. However, there may be technology bridges to help pav the way and solve for some of core objectives behind the goal to go all digital.

While data and data analytics emerged as a unifying theme across brand protection measures, it was clear that the value is in the insights and actions they provide.

- Data can inform where the impacts of global influences are more prevalent and help leaders prioritize resources needed to address them
- Data can support effective management of the industry trends identified
- Data can help resolve some of those legacy challenges subject matter experts have battled over the years

The findings highlighted a desire to invest more in data and advanced analytics, and there are already solutions and practical steps available.

Technologies to capture data become a key enabler to making progress a cross collective efforts.

- For example, physical-to-digital technologies where “intelligent” serialized tokens are coupled with track & trace capabilities. Build in data capture and accrual as part of a solution.
- De La Rue has seen this effectively employed by both governments and enterprise organizations through our Traceology platform and DLR Validate solutions, where both provide data analytics for brand managers.
- We’ve seen these types of technologies are also effective at engaging users because it’s now available on most mobile applications. Data capture technologies also enhance the brand experience and give brand protection teams what they need to enforce their organization’s IP. This is data at scale.

Insights suggest that counterfeiters are taking advantage of gaps created by the relatively low level of collaboration within an organization as well as across the industry. There is an opportunity to be more effective and reduce gaps that are regularly exploited, by more fully leveraging data sources, implementing more advanced analytics capabilities, and facilitating collaboration,

Partnerships to share data could enable broader, mutual benefits across the business.

- Partnerships can be internal, such as in support of corporate sustainability initiatives. Brand protection could share data collection expertise with the business, along with data per se, on the movement of product throughout the supply chain
- Partnerships can be external, among vendors and channel partners, whose combined data sets could enable end-to-end visibility of a product’s journey. These could be direct strategic partnerships or facilitated by a neutral third party, where everyone agrees to treat proprietary data appropriately

The dynamics of the global marketplace are driving the need to think of programs, technologies, partnerships, and business differently. This qualitative study provided some initial insights into key considerations for change.

De La Rue appreciates AGMA’s co-sponsorship of this project and thanks its representative members for participating in the study. *De La Rue and FiveBy welcome your feedback, comments on what would be of further value, questions on any element you’d like more information, and opportunities to discuss how we can support your brand protection programs. Contact Sherri Erickson Sherri.Erickson@DeLaRue.com or John Solheim JohnSol@FiveBy.com with any inquiries.*

Research methodology

Approach

To complete its assessment of how AGMA members use various technologies and methodologies, FiveBy assembled a team of subject matter experts (SME) who were most capable of engaging experienced brand protection professionals in meaningful and informative conversations. This team conducted hour- long, in-depth qualitative interviews between May and August 2020, with twenty industry leaders representing companies that operate in various regions around the world, including Cisco, De La Rue (DLR), Hewlett Packard (HP), Hewlett Packard Enterprise (HPE), IBM, Juniper, Microsoft, Tech Data, and Texas Instruments.

Discussions followed a consistent line of questioning focused on current industry trends, actions taken by thought and technical leaders, and the overall impressions these experts had regarding the state of brand protection. Interviewees were informed about the purpose of the project and objectives of the conversation. To encourage candor, participants were provided assurances of anonymity and confidentiality when sharing any proprietary information.

The composition of interview participants was not homogenous, but rather represented a wide range of roles and responsibilities within their respective businesses ranging from investigations to operational accounting to supply chain management. Although the representatives' businesses are all members of the technology industry, their respective customer focus and product lines vary greatly. Approximately two-thirds of the participants interviewed focus on proactive prevention and mitigation while one-third focus on investigations. Interestingly, another common thread amongst the participants is their long history of experience in the counterfeit, gray market, and fraud prevention space. Most of these leaders have been in their role or similar roles ranging from 7 to more than 20 years.

This purposefully selected group of participants enabled us to build insights into the challenges, interests, and trends that affect brand protection and mitigation across the industry without bias of single role titles or lines of business. Responses were naturally biased toward their specific roles, but in aggregate, the interviews do not portray a comprehensive single point of view or specific trend but rather, enabled identification of general themes and new or lesser-known areas of concern or interest that could warrant exploration. Interestingly, a byproduct of the interviews was the participants gleaning real time insights based on the questions posed. Anecdotally, these reactions suggest facilitation of further communications and collaboration could benefit the AGMA community.

The results of this qualitative study are not statistically validated in this first phase due to sample size and composition of inquiry. Rather, the intention was a discovery of key insights, challenges, and gaps for potential further investigation.

Research Team

Alex Kochis – The founder of FiveBy, a ten-year-old consulting and services company focused on the areas of antipiracy, antifraud, data analytics and forensics for companies with intellectual property-based products. Alex is also the former Director of Antipiracy at Microsoft, previously responsible for HowtoTell.com, and large scale antipiracy and genuine software program development including Product Activation and Validation capabilities and features.

John Solheim – A subject matter expert for the Microsoft OEM supply chain. John led the Microsoft global team and managed authorized replicators and the De La Rue relationship from a supply perspective between 2007 and 2013.

Angela Stanton – The project management lead. Angela managed channel focused anti-gray market, anti-counterfeiting, and software asset management (SAM) initiatives at Microsoft and between 1998 and 2003. She then directed a team of project managers, designers, and developers at a Microsoft SAM partner, between 2007 and 2017.

Supporting Team:

- Cori Hartje
- Todd Hendricks
- Willis Hughes

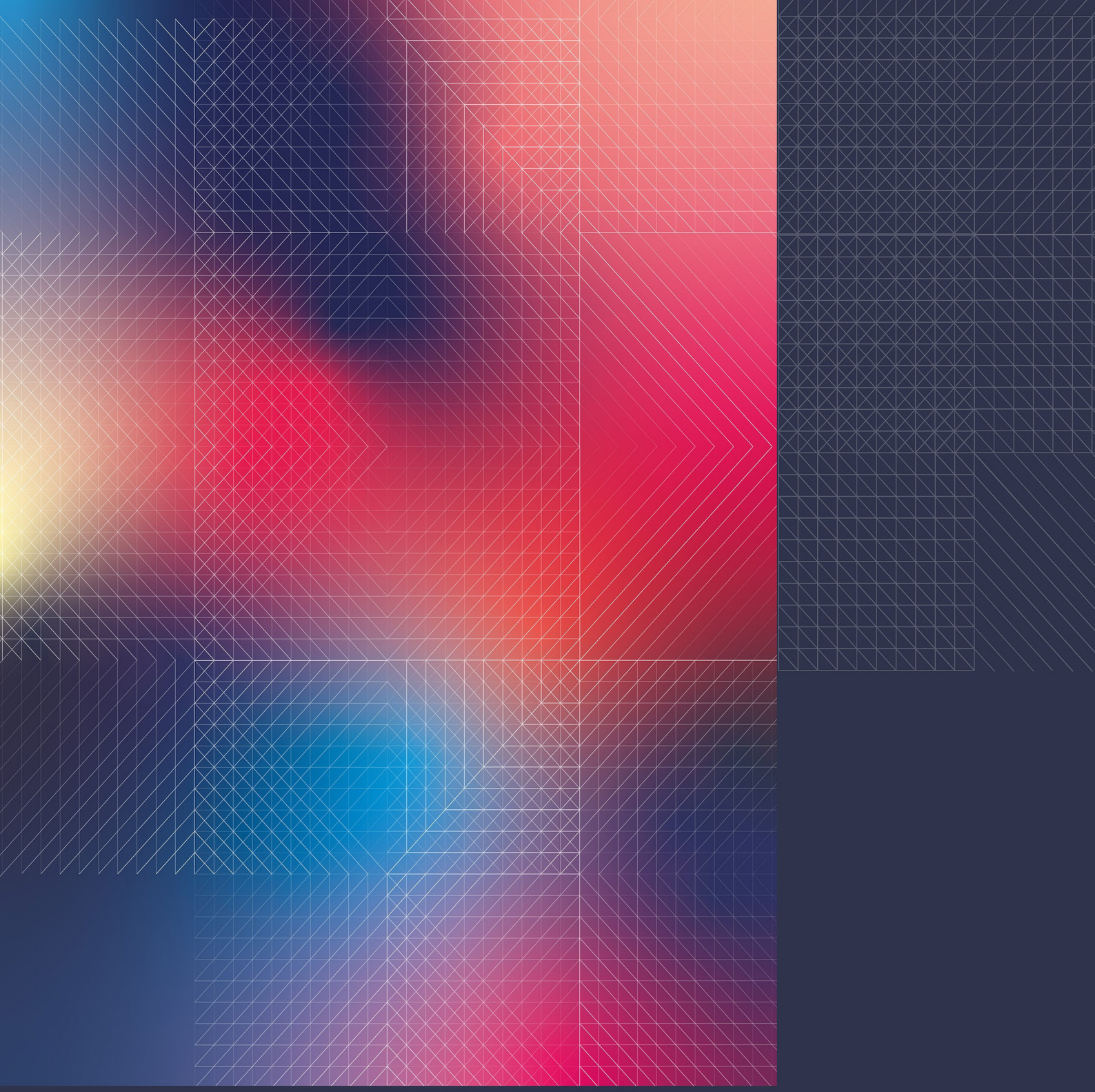
About FiveBy Solutions, Inc.

FiveBy Solutions is an industry-leading security consultancy based in Seattle. Established in 2010, FiveBy works with leading technology companies to identify and solve critical fraud, piracy and compliance issues. Our success is driven by helping our clients turn business risk into business growth.

[1] Combating Trafficking in Counterfeit and Pirated Goods. (2020). US Department of Homeland Security. Retrieved 2020, from https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf

[2] What are the Penalties for Breaking OFAC Sanctions? (2020). New York: Dow Jones.

[3] Yusuf, Z., Bhatia, A., Gill, U., Kranz, M., Fleury, M., & Nannra, A. (2020, August 21). Pairing Blockchain with IoT to Cut Supply Chain Costs. Retrieved November 24, 2020, from https://www.bcg.com/publications/2018/pairing-blockchain-with-iot-to-cut-supply-chain-costs



Thank you