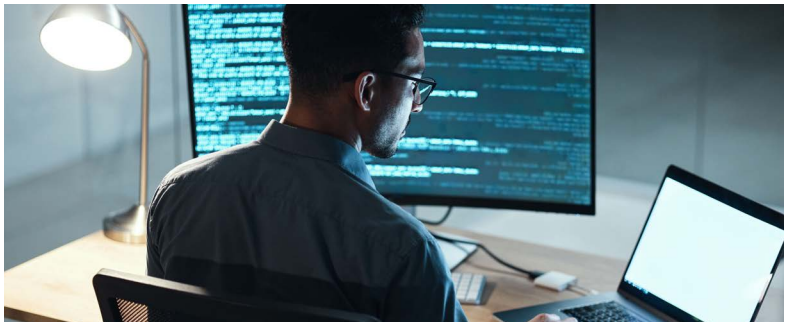
BRAND SAFETY ALLIANCE

DOMAIN PROTECTION REPORT

2025

Table of Contents



Foreword

Welcome to the Brand Safety Alliance's inaugural Domain Protection Report.

This milestone marks not only the first release of our new online brand protection publication, but also celebrates one year since the launch of GlobalBlock – the largest domain blocking service on the market.

In just 12 months, GlobalBlock has helped thousands of brands from all over the world and in dozens of industries to improve their brand protection coverage and reduce the operational burden of domain protection strategies.

What's more, this is just the beginning. The expert team at the Brand Safety Alliance is committed to further enhancements for GlobalBlock in the near future and developing new products and services to assist brands even further.

In this report, we:

- Explore various topics regarding the world of online brand protection
- Provide you with data-driven analysis of GlobalBlock's performance and outcomes across the first 12 months
- Interview Brian Beckham from the World Intellectual Property Organization about key industry trends
- Interview Brian King from RWS who shares his insights about proactive strategies for localization and brand protection
- Share valuable insights from a range of key brand protection leaders on how GlobalBlock has impacted their customers since launch.

In subsequent editions, we will continue to deliver similar informative content as we further the Brand Safety Alliance's mission to collectively help organizations to protect their online assets and create a safer internet for brands and consumers.

Forming the Brand Safety Alliance has been a remarkable journey and we are most grateful for the support and positive reinforcement of our customers who tell us daily how we've been able to help them solve real business challenges, save money and improve operational efficiencies.

We hope you enjoy this report and welcome your feedback on how we can continue to make it valuable and engaging.

If you have any questions or would like to learn more about the Brand Safety Alliance or GlobalBlock, you can contact us at hello@brandsafetyalliance.co or via the GlobalBlock website www.globalblock.co.

Sincerely,

The BSA Team

Feature Interview

Brian Beckham, WIPO

The Brand Safety Alliance spoke with Brian Beckham from the World Intellectual Property Organization (WIPO) Arbitration and Mediation Centre to discuss the evolution of domain name disputes, particularly the impact of the COVID-19 pandemic and the increasing sophistication of cybercrime.

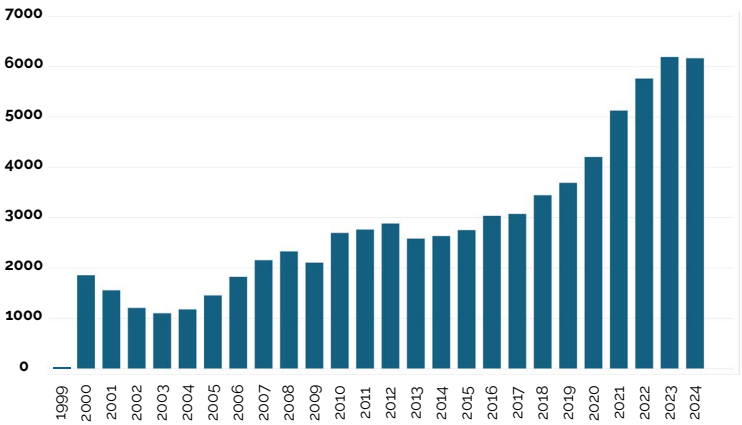
Based in Geneva as the Head of WIPO's Internet Dispute Resolution Section that operates the widely adopted Uniform Domain Name Dispute Resolution Policy (UDRP), Brian is a highly regarded industry veteran and a regular attendee and speaker at a range of trade events including INTA and ICANN meetings.

The world of online brand protection is unpredictable and ever-changing, and no one could foresee the sustained impact of a global pandemic on infringement rates and cybersquatting cases. Cybersquatting is the practice of registering, trafficking in, or using a domain name with the bad-faith intent of profiting from the goodwill of someone else's trademark. WIPO created the UDRP in 1999, and is the global leader in case administration services.

The COVID-19 pandemic served as an unexpected catalyst for cybercrime. While many brand owners had to drastically cut budgets and many predicted a downturn in enforcement activity, Brian notes, "we were slammed with cases because everybody went online."

This mass migration to e-commerce, e-learning, remote work, and communications created a fertile ground for infringements, leading to a surge in cases for WIPO in recent years and a sustained high level of malicious online activity.

Total Filed Domain Dispute Cases Annually



Source: WIPO Domain Name Disputes Statistics, February 2025

The nature of online threats is also becoming increasingly sinister. When Brian joined WIPO in 2007 as a case manager, it was the heyday of pay-per-click advertising. Moving beyond petty annoyances, Brian says a significant portion of cases now involve outright illegal enterprise – by some estimates almost a quarter of cases nowadays.

"That might be fake invoicing, identity theft, fake login pages, phishing, scamming people's credentials, or other malicious behaviour."

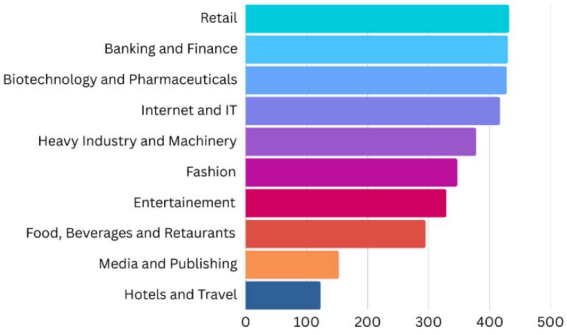
A particularly worrying trend is the targeting of internal company systems. Cybercriminals have begun registering domain names that mimic internal login portals (e.g., hr.company.TLD or benefits.company.TLD) to steal employee credentials in an attempt to gain access to systems. This form of 'corporate sabotage' is a relatively recent development in terms of dispute cases, with some arising in the last couple of years.

Brand owners are struggling to keep up with these threats. Limited budgets force them to make tough choices about which infringements to pursue and some may only have the resources to address a fraction of what they detect. The situation is further complicated by the difficulty in assessing the true risk posed by newly registered domain names.

"No one is immune to this," says Brian.

"We get a lot of filings from companies in the financial services and IT services industries, but no one sector is being targeted at the exclusion of others."

Top 10 UDRP Case Filings by Industry



Source: WIPO Domain Name Report 2024

"There are also domain name registration trends that follow events in the news." For example, in the past year or two, many brands have faced cybersquatting in the .AI ccTLD given the rise of Artificial Intelligence products.

The emergence of artificial intelligence (AI) is also a game-changer in another way. Cybercriminals can now conjure up convincing websites with alarming speed. As the tools become more widespread and sophisticated, brand owners face greater challenges in detecting and combating malicious activities.

Brian champions the need for proactive measures to combat cybercrime. With another round of new TLDs on the horizon, WIPO and the ICA have convened a group of experts to explore options to adapt the UDRP to be quicker and cheaper in addressing certain types of fraud cases.

"One of the big questions that comes up is, does the UDRP continue to scale when cyber criminals have cheap AI tools at their disposal?

"Then the natural progression is a hope that we can make the UDRP even better - but at the same time it must be asked what could be done to prevent some of this from happening in the first place? A growing number of ccTLDs are deploying algorithms to detect actual or potential abuses with good success."

That also raises the idea of proactive domain blocking as one possible opportunity for brand owners to take back some level of control.

Ultimately, the goal of policy makers should be to foster a more trustworthy online environment. This means ensuring that domain names aren't weaponized for fraud and that users can have confidence in the websites they visit.

"We all have an interest in trust on the internet," he says.

Cybercrime Glossary

Phishing – A cyberattack where scammers impersonate a trusted company (such as a brand, bank, or government agency) to trick people into revealing sensitive information like passwords or financial details, often via email or fake websites.

Smishing – A form of phishing that occurs via SMS (text messages). Attackers send fraudulent messages that appear to be from a legitimate source, often containing malicious links or urging recipients to take urgent action.

Typosquatting – Buying domain names that are just a typo away from real brands (like "amaz0n.com" instead of "amazon.com") to fool people into visiting fake sites, stealing data, or pushing scams.

Domain Spoofing – Creating a website that looks almost identical to a real brand's site, usually to trick people into handing over sensitive info or clicking on malware.

Cybersquatting – The act of registering, selling, or using a domain name that closely resembles a trademarked brand or business, usually to sell them back for a profit or use them in bad-faith ways, like scamming customers.

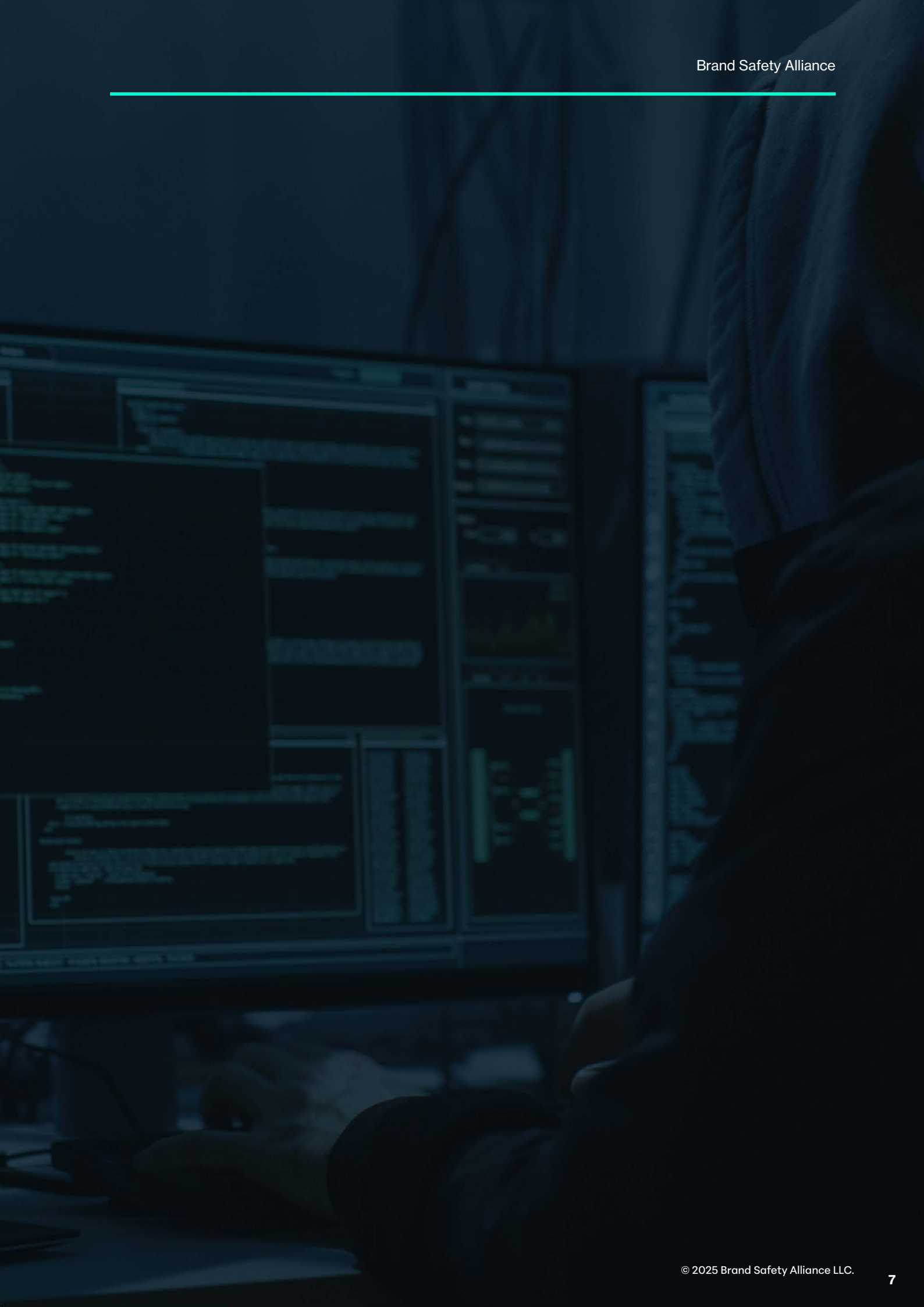
Business Email Compromise (BEC) – A sophisticated scam where attackers impersonate executives, vendors, or partners to trick employees into transferring funds or sharing sensitive data, often using domain spoofing or lookalike email addresses.

DNS Hijacking – A cyberattack where criminals manipulate the Domain Name System (DNS) to redirect users from legitimate websites to fraudulent ones, often to steal credentials or distribute malware.

Reverse Domain Hijacking – When a company or individual tries to unfairly claim a domain name through legal action, even though they don't have a legitimate trademark claim.

Homoglyph Attack – A tactic where cybercriminals register domain names using visually similar characters (e.g., "paypal.com" vs. "paypa1.com" or Cyrillic/Unicode characters) to deceive users into thinking they are visiting a legitimate site.

Drop Catching / Expired Domain Exploitation – Quickly registering expired domains that once belonged to trusted businesses to take advantage of their past reputation, backlinks, and traffic, or to resell them at a high price.



Analysis - Priority AutoCatch in Action

Priority AutoCatch is GlobalBlock's premier value-add feature, helping brand owners seize exact match domains that were previously held by bad actors when they become available.

What's more - this service is included at no additional charge for all GlobalBlock customers and happens in real time providing brand protection around the clock.

In our first year of operations, we've caught almost 10,000 names for brand owners - and added them to their GlobalBlock account free of charge while they sleep.

Needless to say, this feature is highly valued by GlobalBlock customers and we are extremely pleased to have caught prominent names for our clients such as:

tommyhilfiger.shop
ally.life
chase-bank.support
jpmorganchase.vip
godaddy.zip
googlecloud.solutions
microsoft.services

Insights - Expert Feedback from GlobalBlock's First Year

Across our first year protecting brands from imitation and online IP infringement, GlobalBlock has built a strong community of brand protection agencies and domain management experts as partners to bring the service to global corporations.

We spoke to leaders from some of these key organizations to understand their views on domain blocking, the risk landscape for brands online and how the market has responded to GlobalBlock, including:

- Bonnie Wittenburg, Head of Strategic Advice and Consulting at Markmonitor
- Phil Lodico, Head of GoDaddy Corporate Domains
- Stuart Fuller, Chief Commercial Officer at Com Laude
- Lillian Fosteris, Head of FairWinds Partners

Bonnie Wittenburg

Phil Lodico

Stuart Fuller

Lillian Fosteris

What notable changes or consistencies have you seen in brand protection and domain names since we last spoke?

- **Bonnie Wittenburg:** The complexities grow each year. There's a lot going on in the world leading people to think more about security issues and brand protection. What I once considered two distinct buckets are melding: what is the world doing to protect its infrastructure, and what are brands doing to protect their name? The need to protect one's brand is a security play—strategizing how to protect a brand's domain names is as important as prioritizing what domains to actively use, and it's being a good steward to a brand's consumers. Awareness of the need for brand protection is increasing, and steps are being taken, such as with the NIS2 Directive. Now, we interact with our clients' security personnel just as much as with their legal and marketing teams.

  At the same time, brands are increasingly brand conscious. Many are having to rationalize costs and that impacts domain portfolios and the use of monitoring solutions instead of deeper defensive domain registration strategies. Once they've identified what 'really' needs to be protected, they make sure to have locks in place to protect all that qualifies. It's a 'back to basics' approach of prioritizing brands or assets and assigning a monetary value to them.

- **Stuart Fuller:** With the emergence of more Web3.0 extensions, certain brands are keen to protect themselves in that space. They want to understand who could be using their IP in the Web3.0 space–and they want us to tell them what's out there and who's registering what. We talked to a lot of clients who raise the threat of AI, but without really understanding what that means. It's certainly a buzzword that is prevalent at the moment.

- **Phil Lodico:** Overall, we continue to see the same persistent forms of cyberattacks and brand infringement, including phishing, typosquatting, and domain exploitation. While these tactics remain prevalent, mitigation strategies have largely stayed the same. With the exception of GlobalBlock, the industry remains predominantly reactive, with most solutions only being deployed after an attack or infringement has already occurred.

- **Lillian Fosteris:** While corporate concern around third-party registrations in new TLDs has reduced, brand protection particularly in ccTLDs has remained a challenge. With limited availability of domain registration information (i.e. WHOIS), and inconsistent dispute mechanisms, it is often very difficult or impossible to recover domains registered by third parties.

What do you predict for the next 1-3 years in this space?

- **Bonnie Wittenburg:** The security measures taking place, particularly in terms of infrastructure, will continue and likely ramp up. CISOs will have more involvement in domain name management from a security perspective. Justification of domain portfolio sizes continues to come up with our clients and there will be changes to the approach in general, based on technology changes and the increased demand for automation. With AI influencing the way customers use the internet, it will also impact the way brands need to be protected. I think the best place to begin will be to take a rational approach of 'these are the brands, this is their value, here's where we're going to market them and here's where the risks are.'

- **Lillian Fosteris:** I believe the space will remain fairly steady in the next few years with many of the same challenges persisting. Following the next round of new TLDs, I think brand owners will make less and less distinctions in their defensive registration strategies between round one, round two, legacy TLDs, ccTLDs and so on. I don't think the focus on defensive registrations will be as high in this next round as it was in the first.

- **Stuart Fuller:** I think especially going into the second round of new TLDs, there will be more brands looking for tools with Web3.0 and Web2.0 interoperability. We know there's going to be applications that relate to crypto and Bitcoin, for instance. There is always going to be a threat of domain abuse, potentially infringing registrations that are created by an AI engine, but I think one of the good things that will come out of it is Registrars and Registries playing a much bigger part in managing abuse and looking for those trends that are caused by AI in a cyber poacher-turned-gamekeeper way.

- **Phil Lodico:** The two most significant shifts on the horizon for the domain and brand protection space are the next round of TLDs, expected in early 2026, and the increasing integration of AI into the marketplace. The last time ICANN expanded the namespace in 2013, we saw strong brand participation, with over 600 dot-brand applications, alongside a surge in defensive and fraudulent registrations. While I anticipate fewer brands will apply for their own dot-brand TLDs this time, similar patterns of defensive and fraudulent registrations are likely to emerge. Given that each TLD can set its own rules and pricing, I expect to see incentive-based pricing structures designed to drive rapid new registrations. This dynamic will require major brand owners to develop proactive and defensive strategies while leveraging all available tools to protect their brands and customers.

  On the AI front, I anticipate companies will increasingly harness new technologies to enhance decision-making and efficiency, making it easier to achieve their brand protection objectives. AI-driven solutions have the potential to streamline monitoring, improve risk assessment, and optimize enforcement efforts, ultimately strengthening brand security in an evolving digital landscape.

What has the response to GlobalBlock been from brands? Do you have any insight into how it's being used? Has anything surprised you?

- **Phil Lodico:** Brands have been combating domain name abuse for decades, making them more open to exploring proactive solutions like blocking. These approaches not only enhance brand protection but can also offer cost savings compared to excessive defensive domain registrations.While some may view the price point as high, the return on investment has been significant.

One of the most surprising advantages has been the success of the auto-catch feature. Though not widely recognized, many customers have secured valuable domain names in key extensions through this drop-catching capability. In several cases, the value of the domains being secured or blocked has exceeded expectations, reinforcing the strong ROI and making the investment well worth it.

- **Stuart Fuller:** To us one of the key selling points has been the ability to go and block a lot of extensions together–particularly Web3.0–for a cost-effective price. You know there's peace of mind there and that's invaluable to many brands. The clients who've started using it have really appreciated it, and particularly some of the value-add features like Priority AutoCatch are a really good service for them.

  It's also been satisfying to see consistent growth in the number of TLDs taking part in GlobalBlock, particularly for some of the bigger brands that really need to protect their IP across multiple jurisdictions and territories. That's where adding ccTLDs that may be niche in terms of volume or policy complexity can really become key.

- **Lillian Fosteris:** The response has been really positive. Corporations in general prefer the idea of blocking over individual registrations because of its ease, simplicity and potential cost savings. It has been a learning journey for us and for brands because it is a new approach, with evolving offerings and updates over time. Priority AutoCatch has been a consistent highlight for brands, with many pleasantly surprised by its capabilities.highlight for brands, with many pleasantly surprised by its capabilities.

- **Bonnie Wittenburg:** The response has been measured but positive. There's definitely been significant interest where brands can afford it. There is some hesitancy based on other historical blocking products that haven't met expectations so customers are really keen to see some longevity and increasing coverage over time. When we go over the value with clients and explain how they can save costs by letting defensive domains lapse, they immediately get it. People are looking at it as a great new part of their toolkit and a cost-effective measure.

What is your perspective now on the role domain blocking can play in brand protection?

- **Stuart Fuller:** I recently wrote about the five pillars of domain security and brand protection. And they are choosing the right Registrar, locking your most valuable names, implementing domain name monitoring, choosing a reputable DNS provider and, using GlobalBlock. So to us, it's a fundamental, and cost-effective part of a brand protection strategy. Some brands will spend hundreds of thousands of dollars a year on IP protection solutions. These are valuable, but if you think about it from just a domain perspective and consider counterfeit websites, fraud, phishing– for a fraction of that cost you can address those five key pillars and see the impact rather than just relying on the expensive solution.

- **Bonnie Wittenburg:** GlobalBlock is a big part of the total picture. It won't replace other tools but it's one of many that customers can use, and it will augment other tools such as monitoring solutions. It's affordable enough to be a viable option and anything that will inhibit the activity of bad actors in a cost-effective way for the brand is valuable.

- **Lillian Fosteris:** I think blocking can certainly be a key tool in your toolbox. It offers efficiency and streamlines the management process with one purchase, one renewal and so on, without having to manage multiple registrations.

- **Phil Lodico:** Domain blocking is a tool in the kit of protecting one's brands and ultimately one's consumers. While not a panacea, using all available tools, including blocking, defensive registrations, as well as brand monitoring services and relevant take downs give you the greatest opportunity to mitigate risk. Even with moderate benefit, the benefits greatly outweigh the costs associated with blocking.

What disadvantages or challenges does blocking still face?

- **Stuart Fuller:** Clients are asking about how blocking products will cover TLDs launched in the future, such as in the next round. Some are really geared up for that but it's a known unknown–who will apply for what and how impactful will they be? I think it was clear from early in the process of GlobalBlock to see where it could add value to the next round, and the benefits for both brands and TLDs. With a blocking product you can have the benefit of Sunrise protections, as well as ongoing protection as well, and that's a key differential.

Sometimes the challenge is getting the product in front of the right person. Some bigger organisations will have a domain manager and they don't necessarily see the connection yet between purchasing a block and reducing their defensive domain portfolio. Despite the drive to reduce budget every year, that connection isn't always happening.

- **Lillian Fosteris:** One of the challenges is just around timing. It's still somewhat reactive,in that there are spaces that already have a number of third-party registrations and the block can't supersede those. As with any new approach or product,there's also a fear or concern about what may happen if GlobalBlock goes away, and what that means for blocked domains.

  In general, brands are very wary to let domain names lapse, even with a block in place. This is a long-held practice and has made some more reluctant to take up the cost-savings offer of GlobalBlock by opting to block instead of holding on to defensive registrations.

- **Phil Lodico:** The initial iterations of blocking have proven beneficial, but the biggest challenge remains the prevalence of infringing domain registrations that involve variations of key brand names. This includes typographical variations and combo-names—such as "brand + category" or "brand + account"—as well as typos of those combinations, which continue to be heavily exploited.

  While these types of abuse are more challenging to address, there is a growing need to develop proactive solutions that prevent the registration of strategically targeted variations of brand names. Exploring new methods to anticipate and block these types of infringements remains a critical priority.

- **Bonnie Wittenburg:** Cost controls, demonstrating the long-term value and longevity of the product and the introduction of new TLDs will be the biggest hurdles for blocking products moving forward. Blocking has many advantages, but sometimes the challenge is that the people who see and recognize its value aren't the same decision makers who can approve the budget.

Where would you like to see GlobalBlock evolve next?

- **Lillian Fosteris:** Continuing to expand coverage into more extensions, particularly those that have fewer dispute resolution options so it's harder to recover domains, or where it can be challenging to register. It would also be great to have the ability to tailor blocks or select extensions to protect–such as those specific to certain industries or regions. Some brands don't believe they need GlobalBlock's full protection but would be interested in a subset at a slightly lower price point, for example.

- **Phil Lodico:** Beyond my feedback on expanding the range of variations being blocked, I know customers would appreciate a more detailed feedback loop to better understand how GlobalBlock is working for them in practical terms. They want insights such as: How many domains have been protected? How many were intercepted? How is GlobalBlock actively safeguarding my brand beyond serving as a defensive measure?

  We live in a KPI-driven society, and demonstrating GlobalBlock's return on investment is critical to its long-term success. Providing clear, quantifiable insights will be key to reinforcing its value. These initiatives would also be a great opportunity for the Brand Safety Alliance to dive deeper and equip customers with meaningful data on the business impact of their brand protection efforts.

- **Bonnie Wittenburg:** Growing coverage into larger namespaces, including ccTLDs, would be beneficial. The more of the highly abused extensions and the top 100 or 200 TLDs that GlobalBlock can protect, the stronger a case it would make. GlobalBlock has been a really valuable service for our clients and has helped them to receive broader coverage than what would be affordable through a defensive registration strategy.

- **Stuart Fuller:** : It's been satisfying to see consistent growth in the number of TLDs taking part in GlobalBlock, particularly for some of the bigger brands that really need to protect their IP across multiple jurisdictions and territories. That's where adding ccTLDs that may be niche in terms of volume or policy complexity can really become key.

Feature Interview

Brian King, RWS IP Solutions

The Brand Safety Alliance spoke with Brian King from global trademark and patent translation service leader RWS to discuss the importance of a proactive approach to managing often overlooked elements of your business in a global economy.

Based in Baltimore, Brian is the VP of Client Relations for RWS and a practicing Attorney with decades of experience in brand protection and trademark services. He has worked with some of the world's most prominent organizations and assisted many global brands during his tenure.

While the internet has made global reach easier than ever for organizations and driven an ecommerce industry expected to be upwards of USD7 Trillion in 2025, consumers have ever-increasing demands of companies to engage with them in their own languages with culturally sensitive and relevant messages beyond just the basic products and services.

Brian observes "the internet and related technologies make globalization much more possible, and simultaneously I've seen increased need for localization, meaning customers want to be met where they are. Brands that have been able to do this have not only enjoyed greater revenue and overall success, but avoided the significant costs related to failed product launches and new market exploration."

From a domain perspective, this impacts the extensions and types of names a corporation needs to reach customers 'where they are.'

Owning ccTLDs is part of this, and local content in many countries requires the use of ccTLDs. It's an expectation of the market in many places in the world."

In this environment, Brian believes it is crucial to get on the front foot and think ahead for future business and market needs.

"It's important to be proactive. It's fun to play offense and our clients find it helpful," he says.

"Companies should think about localization proactively, whether that's website content or even internal materials, because it saves a ton of time and money after the fact."

Failing to plan for localization can lead to significant financial and timeline setbacks.

"We have seen clients spend hundreds of thousands of dollars to develop content they hoped would be useable for a global audience, only to find when it came time to translate or localize, it simply wasn't possible.

"The content would need to be redeveloped for certain markets and geographies—and the time and cost impacts of that are very real."

Brian highlights brands often treat domain registration as secondary to trademark registration, to their detriment.

"Every corporate registrar has a nightmare story about a client who waited until the last minute to register their domains in various ccTLDs and gTLDs and was scrambling, after naming a product or having a press release, needing to acquire or quickly register domain names all around the world."

To combat this need, Brian emphasises the importance of corporate registrars continuously educating their clients on industry developments and new tools.

"Even the savviest domain name administrators require constant updates and education on the developments in the industry," he says.

"It's a space where you thought you knew something last year, and then the next year the landscape is tremendously different.

"Tools like GlobalBlock are a great example of the need to continue educating clients on best practices for defensive registrations, blocking, monitoring and enforcement.

"I wish something like GlobalBlock existed back in my corporate registrar days. I think it will be a tremendous tool in the toolbelt for brand owners because of the broad coverage and the ability to block upfront, then unblock as business expand into new markets down the road."

BRAND SAFETY ALLIANCE

For more information, visit brandsafetyalliance.co or contact a Brand Safety Alliance representative at hello@brandsafetyalliance.co