The enemy within: combating internal counterfeiting

The increasing risk coming from within organisations should not be underestimated. However, developing resilient policing and reporting strategies can help to counter these internal threats

AUTHORS
JULIAN GRIJNS AND SAM TAYLOR

Almost all industries are subject to potential fraud from counterfeiters but the increasing risk of such threats coming from within your own company cannot be overlooked by corporate boards.

While cybersecurity breaches and data theft receive the most headline coverage, counterfeiting of goods or intellectual property – which has been a staple of the post-industrial world for nearly 100 years – remains prevalent and pervasive. Such counterfeiting applies not only to big-box retailers or manufacturers, but also to small family-owned or start-up businesses, many of which are ill equipped to respond. In some cases, such businesses are completely unaware that their intellectual property has been compromised. Companies need to take such threats seriously and to build countermeasures into their business plans. Industries which are particularly vulnerable to internal counterfeiting include garment manufacturers, mobile application developers, financial technology firms and any industry operating or contracting to a manufacturing facility in a developing world market.

Favourite insider tactics: overproduction and diversion

The garment and accessories industry is well known for significant levels of counterfeiting and product diversion, sometimes emanating from internal sources. Direct counterfeiting in the apparel industry is ubiquitous – although contract violations can be even more common. The overproduction and subsequent diversion of imperfect products can be considered a gateway to direct counterfeiting; for contract manufacturers and the local third parties that support them, it is one of the easiest ways to profit illegally from brand owners.

In one recent case, Kroll was approached by a client which had discovered that its legitimate products were being sold in unsanctioned sales channels.

PICTURE: FRANKIE'S/ SHUTTERSTOCK.COM

Beginning with targeted undercover purchases at the retail level and working up to wholesalers, Kroll identified a product diverter in the Middle East which was ultimately sourcing his product from the client's factory in East Asia. An undercover investigation at the factory determined that the local partner was violating certain provisions of the production contract. Instead of burning faulty and excess products, the contract factory was selling them to a network of local parties; these in turn sold the products on to international wholesalers with a history of product diversion. The client's routine audits never identified the violations taking place at the factory.

Hiding in plain sight

Multinational companies spend significant amounts of time and resources protecting their supply chains and the trade secrets embedded within them. This often means sharing information internally with interested parties only and keeping confidential the presence of contracts, designs and manufacturing techniques. The commoditisation of most products has transformed speed-to-market and product presentation into competitive differentiators. There is thus an inherent value in keeping the supply chain secret. Successful counterfeiters embed themselves within this secrecy, often presenting themselves to the market as a legitimate part of the client's supply chain.

Recently, Kroll was retained by a well-known clothing brand to investigate the production facilities and distribution sources of good-quality counterfeit shirts that were arriving in high volumes in Europe from Turkey and China. Having spent years on proactive enforcement in Europe and Turkey, the client found that its efforts achieved only the temporary interruption of the counterfeiters' activities. Leveraging the client's existing intelligence and using a variety of methods – including controlled purchases, human intelligence,

internet investigations and public record data – Kroll was able to map out a highly organised counterfeiting supply and distribution network, identifying over 150 involved individuals, companies, websites or domains, emails, social media accounts and telephone numbers. A significant group had created its own fashion labels and registered a series of front companies to make itself appear a legitimate distributor of the client's brands. Undercover buys determined that this group was effectively moving counterfeit products through Customs under the veil of being a legitimate distributor. An investigation spanning 10 countries and using civil and criminal enforcement actions resulted in the identification of factories, as well as storage and airport distribution facilities, and ultimately to a significant number of arrests and seizures of counterfeit products. After the event, it was determined that several of the counterfeiters were in fact former employees of a garment contractor working with the client.

Counterfeiting is a pervasive problem throughout most industries and there are few companies – no matter what place they occupy within the supply chain – that are not exposed to counterfeiting, or at least product diversion. Samples of counterfeited products or categories with which we have direct experience include condoms, diabetic test strips, automotive parts, building supplies, olive oil, aluminium foil, energy drinks, commercial pumps and valves, and – of course – apparel.

Brand identity sells clothing and accessories. In the apparel and accessories industry, an insignia, label, brand-specific marker or design element is often the only thing that visibly separates one pair of boots from another. As such, counterfeiting has been and will continue to be one of the most significant issues that this specific industry faces. Unlike counterfeited products in commercial, business-to-business industries, retail-facing enterprises have to contend with the largest sales channel of all – the Internet. In one recent case, Kroll worked with an apparel company for three months, helping it to identify and shut down over 8,000 internet domain names which were being used to sell counterfeited sports apparel. Three separate US federal lawsuits resulted in default judgments of over $2.5 billion. The defendants, of course, never made an appearance.

> **There is an inherent value in keeping the supply chain secret. Successful counterfeiters embed themselves within this secrecy**

Assistive technology: advantages and limits

The apparel and accessories industry has long been talking about new anti-counterfeiting technologies, such as radio frequency identification tags, which allow for products to be tracked and traced from production to consumer. However, such technology presents a number of issues, including privacy concerns and production costs. Hologram and authentication technologies have proven successful in this sector, but only to the extent that they enable the brand owner to identify counterfeits. Consumers buying from certain sales channels are still knowingly or unknowingly buying counterfeits.

Effective strategies

The following common-sense measures can be highly successful in minimising the risks of counterfeiting.

Risk-based due diligence

An appropriate level of due diligence rather than a one-size-fits-all compliance approach is essential. The due diligence should include providing the anticipated third party with questionnaires and disclosures, and asking it about the ownership of the company, as well as its regulatory, environmental, legal, tax and other operational history. It should also carry questions dealing with anti-corruption, relationships (eg, whether any principals have direct or indirect ties with local government) and interests by principals in other companies domestically and abroad.

The risks in a certain geography, the size of the potential relationship and the level of access to the brand owner's trade secrets should all be considered when determining an appropriate level of due diligence. Public record investigations alone are often insufficient as some markets have incomplete and unreliable source records. When possible, human inquiries should be used to assess the third party's reputation and track record. Due diligence should not be limited to new relationships but

should be directed to established ones as well. There is a regular tendency by brand owners to become too trusting and complacent about long-term distribution and manufacturing partners. As a result, audits, inspections, and updated due diligence of such trusted third parties can fall by the wayside.

Conduct ongoing monitoring and site audits

Self-certification by third parties that they have read the brand owner's supplier code of conduct, ethics standards and related policies is just paper. Instead, ongoing monitoring and site audits should be conducted on a regular basis. To increase the efficacy of such measures, employees must be empowered to use the brand owner's confidential hotline and reporting structures. This means regularly educating employees on the value of the company's trade secrets, the impact that counterfeiting has on margins and the steps that the brand owner will take to investigate product diversion or counterfeiting (eg, civil lawsuits, seizure orders or referrals to law enforcement).

Brand owners should also conduct both scheduled and unscheduled internal and external audits of their manufacturing facilities, stock inventory and upstream and downstream suppliers and distribution partners – such actions can often uncover instances of missing products which can be enough to launch an investigation. Building out an internal investigative function or working with an outside firm with expertise in this topic will send a signal internally that the company takes these matters seriously and put fraudsters on notice.

Regularly assess market presence by leveraging data analytics

Companies should also conduct regular and formal market assessments to identify and assess counterfeiting or diversion. This can include targeted research to identify rogue websites, mass e-commerce channels and forums selling or promoting the brand owner's products.

Self-certification by third parties that they have read the brand owner's supplier code of conduct, ethics standards and related policies is just paper

PICTURE: FIZKES/ SHUTTERSTOCK.COM

Several companies leverage algorithms and data analytics to crossmatch domain registration data with site contents (eg, images, text, price and metadata) to cluster sites based on common characteristics. This clustering is often highly accurate and allows brand owners to target groups of websites that are likely being operating by the same counterfeiting enterprise.

> **Public record investigations alone are often insufficient**

Companies in the pharmaceutical and beauty products industries have used statisticians to create statistically significant samples of retail and online locations selling the brand owner's products. This should include geography, customer demographic and the type of retail outlet (eg, mass retail or online). Surveys and controlled undercover purchases have allowed brand owners to identify patterns and upstream distributers which are diverting or selling counterfeits. In many cases, this allows the brand owner to map its own supply chain and identify anomalies in distribution.

Bolster physical and information security

The insider threat is among the greatest threats to a company's supply chain. For that reason, physical and information security, as part of a comprehensive risk programme, remains one of the best deterrents. Among physical and information security questions, the following immediate areas should be addressed:

- Do facilities handling sensitive information and production have a keycard control system? Is it monitored and enforced?
- How is facility entry monitored during and after working hours?
- Are surveillance systems used? How are recorded tapes managed?
- Does the facility use metal detectors or other production-related security?
- Are employees provided with regular security awareness training?
- Does the company perform regular physical security assessments?
- Does the company have a confidential integrity hotline? Are employees or third parties trained on its use? Does the company employ other confidential reporting mechanisms?
- How are stale or blemished products and overproduction handled?
- Has the company employed anti-counterfeiting security labels?
- Has the company defined its trade secrets?
- Has an information security assessment been performed?
- Has the company performed any network vulnerability or penetration tests?
- Have user-level access control measures been defined?
- Does the company employ internet and virtual private network logging and endpoint threat monitoring?

- Have the company's HR and IT departments drafted policies and procedures for departing employees, including exit interviews and termination of access credentials?
- Has the company evaluated how sensitive information is shared and stored with third parties?
- How are prototype products shared with third parties?
- Does the company regularly evaluate the marketplace for counterfeits? Does it use online brand monitoring tools (eg, MarkMonitor)?
- Has the company joined any industry anti-counterfeiting alliances, such as the International Anti-counterfeiting Coalition?
- Has the company properly registered its trademarks in the countries where its products are manufactured and sold?

Hardware manufacturers across a range of industries, from automotive parts to mobile devices, have successfully employed anti-counterfeiting programmes which include the strict compartmentalisation of trade secrets within the organisation. Under such programmes, mobile devices are banned from R&D areas, prototypes are colour coded or contain so-called 'Easter eggs' (ie, hidden elements that if replicated in another product indicate counterfeiting) and multi-component devices have a serial number or three-dimensional code printed and sometimes hidden on each sub-component. Critical information documents that must be shared with third parties use data-loss prevention software. In some cases, brand owners have even resorted to using multiple versions of the same documents which each carry a unique and subtle typographical error in order to identify any information leaks across internal departments and outside of the organisation.

Combating counterfeits can appear to be a never-ending game. However, if an organisation develops appropriate internal policies, procedures and – critically – a culture of awareness and reporting around physical and cybersecurity, the task becomes far less daunting. Whether you are a Fortune 500 company with a large annual brand protection budget or a small business with limited resources, arming yourself with the fundamental and common-sense approaches outlined here can help protect your business, clients and brand name. **WTR**

Julian Grijns is a managing director and Sam Taylor is an associate managing director at Kroll
jgrijns@kroll.com
staylor@kroll.com