



TenIntelligence

Due Diligence | Investigations | Protection

Our Services



@TenIntelligence

Our Intelligence | Your Assurance

Vision, Mission & Values

TenIntelligence was created in 2012, with a vision of being an ethical investigation company that operated on the foundations of trust and integrity.

Since 2012, our continued vision is to be a playmaker in our field, an investigation and protection consultancy recognised for our diligence. Our mission is to protect our clients, people and their livelihoods from harm through effective **DUE DILIGENCE, INVESTIGATION AND PROTECTION.**

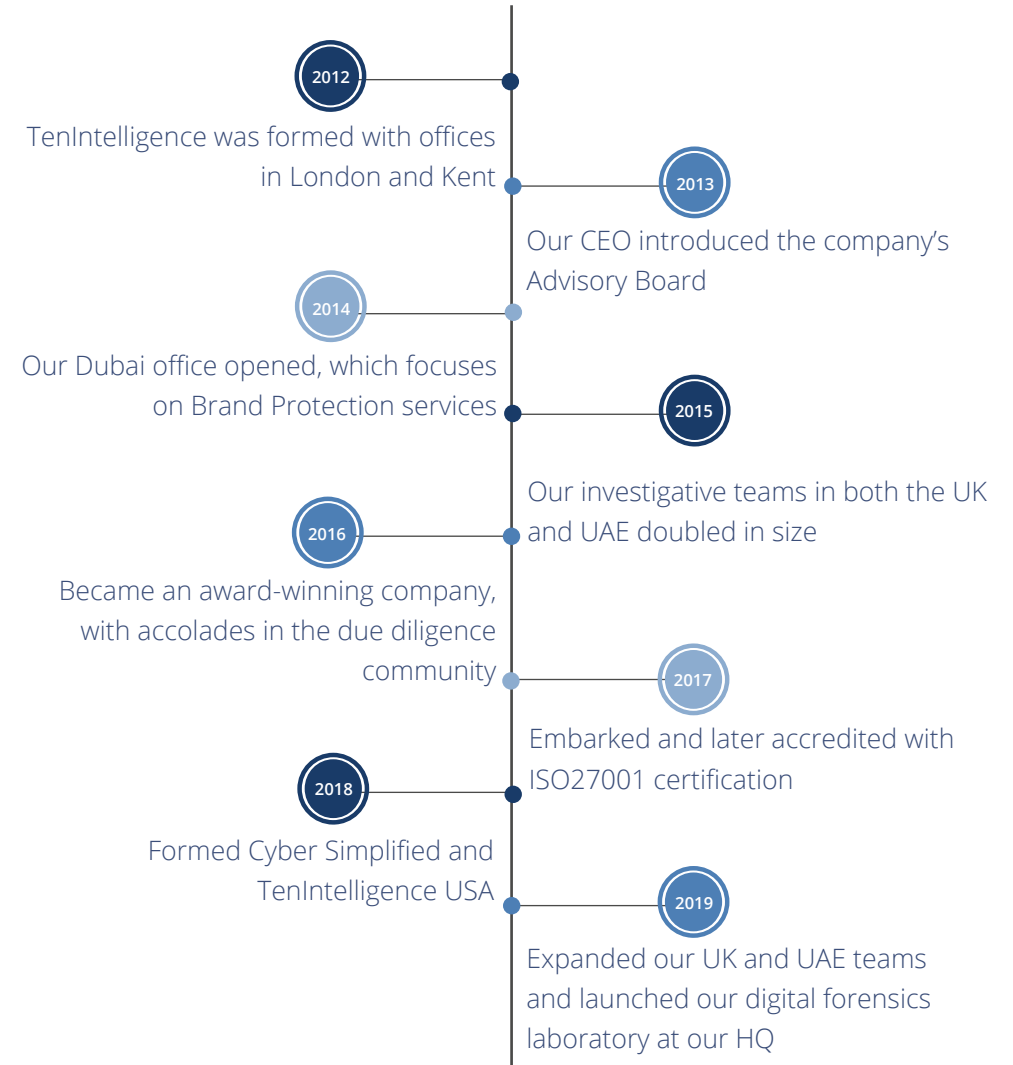
To achieve this, we bring together an experienced, dynamic and multilingual team who possess different skill sets, including legal, cyber security, forensics, brand protection, anti-fraud and compliance experience.

TenIntelligence prides itself on maintaining an outstanding and consistent reputation for excellence, integrity and success, building long term and rewarding relationships with our clients, colleagues and others with whom we do business. We aspire to be a dedicated and exemplary corporate citizen.




Our Journey With You

When choosing an investigation company, you need to be confident that it can meet your needs. Since 2012, TenIntelligence has advised and supported many organisations often through difficult circumstances. We will continue to invest in our team, work closely alongside our clients, while keeping true to our core values.



DID YOU KNOW...?

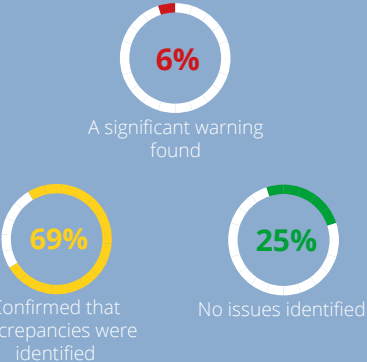
1 A recent UK survey revealed that **10%** of all respondents had admitted to having lied on their CV, with **40%** admitting lying about their qualifications and **30%** lying about their level of experience.
(YouGov Omnibus, 2017)



40% Education/qualification

30% Level of experience

2 Some candidates appear like the ideal candidate at first glance, but turned out to be less than desirable. Of all the background checks TenIntelligence completed into senior executives during 2018, **75%** of the cases identified **amber** or **red** flags, based on our traffic light system. This means that during the open source phase, adverse findings and anomalies were identified which required a further investigative phase.



6% A significant warning found

69% Confirmed that discrepancies were identified

25% No issues identified

3 Using evidence from 237 corruption cases from the last 30 years, Transparency International identified over **£250 billion** worth of funds had been diverted by rigged procurement, bribery, embezzlement, corruption and the unlawful acquisition of state assets across 79 different countries.
(Global Fraud Report 2018 by ACFE)

4 In an ACFE report, 34% of all reported corruption cases were perpetrated by an **employee** who was unusually close to the vendor, supplier or customer.
(Global Fraud Report 2018 by ACFE)

Our **Due Diligence** allows you to work with confidence and compliance.

Assurance

Our team provides clients with the information they require to make assured decisions:

- we interrogate the corporate history of individuals and companies, specifically looking for undisclosed red flags, adverse findings, false or exaggerated statements
- our research covers multiple jurisdictions and is performed in different languages
- we provide clients with unbiased insight and assess the appropriateness of an individual or company based on third-party interviews

Financial Crime Compliance

Our team supports clients to deter financial crime and ensure they meet their anti-money laundering and compliance obligations by:

- providing accurate information on Ultimate Beneficial Ownership, corporate structures and sources of wealth
- determining whether an organisation, or the beneficial owner of an organisation, is a Politically Exposed Person (PEP), conduct ongoing monitoring and report on suspicious transactions
- investigating whether corruption and bribery schemes exist within your organisation, procurement functions and supply chains

Strategic Intelligence

We safeguard our clients' reputation and protect them from geopolitical risks and international regulatory breaches by:

- collecting reliable intelligence on diverse business customs, market entry strategy, fraud risks, corruption levels, political influences and the regulatory environment
- providing competitor intelligence analysis to anticipate competitive threats, product launches, marketing campaigns and expansions into new markets
- guiding senior management through charted territories by securing travel arrangements, through to developing secure and compliant third-party assurance programmes

WERE YOU AWARE...?



49% of global organisations have experienced corporate crime between 2016-2018. *(Global Economic Crime and Fraud Survey 2018 by PwC)*



The total cost of corporate fraud reported globally in 2018 was over **US\$7 billion**, with 22% of these cases causing a loss of US\$1 million or more. *(Global Fraud Report 2018 by ACFE)*



85% of fraudsters displayed **at least one** behavioural red flag, including those who live beyond their means or experience financial difficulties. *(Global Fraud Report 2018 by ACFE)*



Internal control weaknesses were responsible for nearly **50%** of all reported corporate fraud; yet by implementing simple anti-fraud controls, monitoring and surprise audits, all helped significantly reduce losses from fraud. *(Global Fraud Report 2018 by ACFE)*



44% of respondents said they plan to **boost spending** on fighting against corporate fraud over the next two years. *(Global Economic Crime and Fraud Survey 2018 by PwC)*



68% of external perpetrators committing the fraud are 'frenemies' of the organisation – agents, vendors, shared service providers and customers. *(Global Economic Crime and Fraud Survey 2018 by PwC)*

We perform thorough **INVESTIGATIONS** in a secure manner.

If a suspicion of fraud has arisen, we trust our clients' instincts and consult with them to develop the next course of action. We help them analyse the evidence and circumstances surrounding the suspicion and set out clear objectives in an investigation plan.

Corporate Fraud and Litigation Support

Applying the highest ethical standards, TenIntelligence provides investigative services to uncover corporate fraud and help clients find the truth:

- determine the details of the suspected fraud, identify those involved and understand the mechanics of the fraud
- collect, secure and analyse all evidence to strengthen the investigation
- engage with surveillance teams to aid the detection and investigation of fraud
- interview suspects or witnesses to collect supporting evidence
- helping our clients' legal teams and litigators to identify, unravel and recover assets lost to fraud
- review and implement measures to prevent fraud from occurring again

Digital Forensics

Identifying and gathering digital evidence is key to successful litigation and dispute resolution. Our Certified Forensic Practitioners:

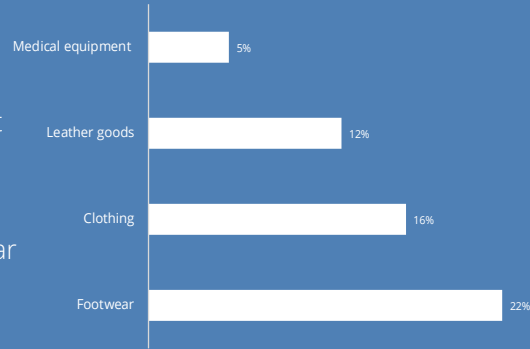
- apply chain of custody, covering seizure, exhibit handling, data collection and preservation through to examination and investigation
- conduct forensic examination, including the imaging (producing a working copy) of all digital data from the devices collected using specialised forensic software and hardware
- work with clients to analyse the data collected, test investigation hypotheses, understand and interpret data structures and present evidential findings

WORLD TRADE IN FAKE GOODS IS NOW RISING...

Counterfeiting and trademark infringements are serious Intellectual Property crimes. Counterfeit food products, electronic goods, luxury items, auto spare parts, tobacco and pharmaceutical products continue to violate the rights of trademark, patent and copyright owners and is a huge safety risk to consumers.

Other counterfeit products, such as motor vehicle parts that are constructed using substandard and weak metals, can also trigger serious malfunctions and cause life-threatening injuries and even fatalities.

The goods making up the biggest share of 2016 seizures worldwide (OECD and the EU's Intellectual Property Office)



For instance, according to the World Health Organisation, poor-quality antimicrobials not only will fail to treat infection, they also contribute to the evolution of antimicrobial resistance, which UK researchers have estimated could kill up to 10 million people a year by 2025.

We offer a truly global reach

Brand protection is one of our key services and with our headquarters based in Dubai UAE, it gives all of our clients a regional presence in the Middle East.

Appointing a "private investigator" is considered illegal in the UAE (and Gulf region), even if you bring a contractor in from another country. If you believe someone has committed a crime, you have the right to request a police investigation who may collect evidence for you. Respecting the regional law and customs is key to successful outcomes.

TenIntelligence has a long, established and trustful relationship with Law Enforcement Agencies (LEAs) in the different Emirates, which allows us to work alongside them collaboratively for the identification and safe removal of counterfeit products.

We are here to **PROTECT** your brand and keep your customers safe.

Our brand protection services begin with **IDENTIFYING** counterfeit and infringing products, followed by carrying out **ENFORCEMENT** action with local LEAs, and having goods seized until issuance is received from the Courts for its **DESTRUCTION**.

Step 1 Identify

- We conduct test purchases to confirm the originality of the products as well as performing due diligence into the suspected traders to identify any associated businesses.
- Our team performs site visits to known and suspected premises to collect trader details, images and descriptions of products and other supporting evidence.

Step 2 Enforce

- With our clients' instructions, we arrange enforcement action and file complaints directly with the relevant LEA.
- We continue to liaise with the LEA to arrange suitable timings for the enforcement and notify supporting logistics companies to attend the raid site.
- During the enforcement action, our team will perform a count on the number and type of products seized, prepare enforcement reports along with supporting witness statements and submit to the LEA.
- Our clients are updated regularly throughout the entire enforcement process.

Step 3 Destroy

- Our work does not stop there, the team will ensure the case is transferred from the LEA to the relevant Court and have the products released and destroyed.
- After attending the controlled destruction process, we provide clients with an official destruction certificate and finalise the enforcement action reports accordingly.

WHAT HAVE WE LEARNT?

Phishing, ransomware and DDoS attacks are often reported in the news. The unstoppable growth and impact of cyber-crime requires organisations of all sizes to rethink their approach to cyber security, helping them avoid financial losses and reducing reputational damage.



In 2018, 32% of UK businesses reported having a cyber security **breach** or attack with 20% of businesses exposed to viruses, spyware or malware.

(Cyber Security Breaches Survey 2019 by GovUK)



In 2019, an organisation will become a victim of ransomware **every 14 seconds**.

(2019 Official Annual Cybercrime Report by ITGovUK)



77% of businesses believe staff responsible for their cyber security have the right skills and knowledge. Yet, **only 27%** of businesses provide cyber security training to staff.

(Cyber Security Breaches Survey 2019 by GovUK)

52% of UK businesses are not fully compliant with GDPR

As stated by the GDPR research 2019 by Egress, **52%** of UK businesses **are not fully compliant** with the regulation. 37% of the respondents had reported an incident to Information Commissioner Officer (ICO), with 17% having done so more than once. 35% of the organisations said GDPR has become **less of a**

priority for them, until the recent huge fine by ICO to British Airways and Marriott.

In the UK, the average cost of a data breach has grown to nearly **£2.7 million** (Cost of a Data Breach Study, IBM). Organisations must have a thorough system in place to protect personal data and avoid being fined.

First ICO action under GDPR legislation against AggregateIQ Data Services relating to the Cambridge Analytica scandal.



£100,000 fine to telecoms company EE for sending over 2.5 million direct marketing messages to its customers without their consent.



£500,000 fine was issued to Facebook for sharing approx. 87 million Facebook users' data to AggregateIQ Data Services without their knowledge.



£183 million fine to British Airways, due to breach of credit card information, names, addresses, travel booking details and logins for approximately 500,000 customers.

Our **CYBER SIMPLIFIED** resources for your complicated cyber threats.



Technology has become an integral part of our personal and business life. Whilst we enjoy the benefits it brings; it is also a highly complicated field with devastating consequences if not used appropriately.

Yet, we know some organisations find it challenging and time consuming to mitigate cyber risk; as well as managing their legal obligation to protect personal information under General Data Protection Regulation (GDPR) and data protection standards. Cyber Simplified is here to guide organisations with jargon-free advice to help prevent cyber-crime and to improve their posture around protecting data and compliance.

Cyber Security

Our team guides organisations through the cyber security process and we will:

- identify critical vulnerabilities with our penetration testing service, providing threat vulnerability and risk assessments
- work with organisations to design and implement preventative and corrective measures, including staff awareness and training programmes
- provide an experienced Chief Information Security Officer (CISO) for your strategic security discussions, board advisory and planning
- audit existing systems, identify immediate threats and provide comprehensive risk assessments

Data & Privacy

For your organisation to become compliant with GDPR, DPA 2018 and other data protection guidelines; we will:

- help audit your organisation's readiness and resilience by testing systems, processes and infrastructure for security soundness
- conduct specific data flow assessments providing gap analysis to identify control weakness, strengths and areas for development
- design and develop a Breach & Incident Response Plan, enabling incident responses to be effectively managed, including staff, third-parties and contractors
- utilise our certified Data Protection Officer (DPO) to act as the incident responder and to review and define your GDPR risks



 **TenIntelligence**
London | Dubai

Due Diligence | Investigations | Protection

CONTACT US

London: +44 (0) 203 963 1930

Dubai: +971 (0) 4333 4669

www.tenintel.com

info@tenintel.com

   @TenIntelligence

ذڪائنا هو ضمانك