CNS RISK
INTELLIGENCE. WORLDWIDE.

INTELLIGENCE & INVESTIGATION

Support for Dispute Resolution, Litigation & Arbitration Matters

CNS RISK

Finding the missing links

Our teams find admissible evidence and produce relevant witnesses in cases where trails are difficult to follow. We use human intelligence and technology previously only available to government agencies to uncover and align critical information, giving our clients clean line-of-sight to the complex risks they face.

- Identification and interview of witnesses
- Gathering evidence to refute opponent testimony
- Finding confidential sources & materials
- Collecting & analyzing intelligence on adverse parties
- Global asset tracing
- Forensic accounting
- Proprietary investigation analysis tool suite

Enhanced Investigation Technology Toolset

CNS Risk's proprietary suite of enhanced investigation tools analyses separate silos of bulk information in one dimension, allowing the identification of immensely complex networks and below-the-surface detail, including corporate listings, telephone records, emails, ISP data, and keycard access logs.

- Unlimited source data acquisition and mediation
- Near real time analysis of source data
- Find, link, chart, map, export and display Target activities, movements and relationships
- Learning capabilities & pattern recognition
- Limitless alarm setting and scenario testing
- Location solution functions, including global geo-location tracking

Case Study I: CEE Aerospace Theft

Client: A UAE headquarted aviation company providing services globally.

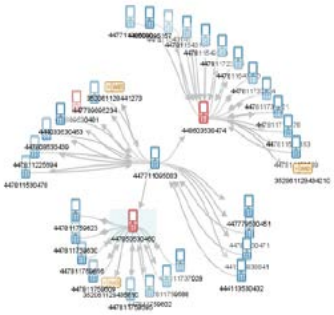
Situation: The client contracted with a group of companies with offshore ties in order to purchase several million euros worth of aviation equipment. The agreed fee was transferred, but the client did not receive all the ordered goods.

Action:

A comprehensive background investigation and tracing of the supplier's assets, its owners and its senior management to support the client during the negotiation and litigation processes.

CNS proprietary technology deployed to sift and analyze hundreds of thousands of mobile phone and email records held by the company in the search for clues and evidence.

Results: CNS collected intelligence on the relevant assets, found compelling evidence of the whereabouts of the transferred funds, and also highlighted a strong suspicion of fraudulent financial activity and criminal behaviour.



Through confidential source inquiries and enhanced investigation data analysis, we were able to pinpoint where the supplier stored inventory and thus locate the undelivered equipment.

Further action: CNS recommended deeper analysis of the offshore ties; however, the client felt that it had sufficient information to enter negotiations from a position of strength.

CNS Risk Enhanced Investigation Technology Tools

The toolset

Based on a decade of on-the-job R&D, CNS Risk has created a high-specification technology suite to support deep-dive investigations.

Commercial clients can now reap the benefit of powerful investigation and analysis tools previously only available to Law Enforcement Agencies (LEAs) and other government security services.

Deep-dive investigations

Proprietary hardware and software is utilised during client investigations, and in collaboration with their counsel and other advisors. Functions include:

- Global open source queries (corporate lists, news aggregators, legal & tax records, etc.)
- Dragnet forensic data mining and analysis of massive datasets (e.g. phone records, emails etc.)
- Seamless integration and analysis of 3rd party data sources
- Counterintelligence applications. (cyber security; counter surveillance measures, etc)

Licensed In-house systems

We also licence bespoke solutions to clients that prefer to run investigations in-house.

We design systems in collaboration with the client and their advisors, and supply training and consultancy services as required.

Case Study II: Illegal takeover of assets in CEE

Client: The founder of a US headquartered international agri-business group with subsidiaries in CEE and FSU.

Situation: Our client learned that his business partners and co-owners were planning an attempt to take over the CEE plant, and to illegally push him out of the firm.

We were asked to find evidence of suspected fraudulent activities at the plant, and to support possible litigation and/or negotiations around this highly sensitive issue.

Action: CNS provided a multilevel action plan and formed a specialist team to find the required information in a legal, transparent manner.

Results: We collected confidential information on the movements and behaviour of the local management and co-owners, and surveyed and reported on the plant's security environment and IT systems.

Our security staff secured the offices, and in the presence of the client, our team entered the facility. Using our investigation toolset, CNS IT and accounting forensic experts pinpointed instances, and found hard evidence, of fraud and deceptive business practices.

Further action: At the client's request, the IT forensics team continued to mine data on devices legally obtained from the facility. Evidence collected during the investigation was successfully used during the negotiation and litigation processes.

Duration of project: Four months

Resources employed: Four investigators; two senior security professionals; ten security guards; three IT professionals; two lawyers; two accounting professionals; three risk advisors.

Case Study III: Russian Counterfeit Ring

Client: A global FMCG group with production and logistics operations in Russia and turnover of around €1 billion in the country.

Situation: Over €80 million sales loss per year owing to a sophisticated counterfeit coffee ring.

Action: Investigations were undertaken in 11 major FSU cities to determine the origins and nature of the criminal ring behind the operation.

CNS Investigation Technology was deployed in order to acquire, analyse and document large datasets of phone, email and other electronically stored evidence. In parallel, forensic accounting methods attempted to trace the ultimate beneficiaries of the crime and its proceeds.

Results: CNS identified the distribution system and main counterfeit production sites.

- We determined that packaging was stolen partly from the original manufacturer and partly counterfeited using imported glass jars.
- Inferior quality coffee was imported from neighbouring European countries at cheap prices, with customs authorities paid off in order to circumvent import taxes.
- The owner of the counterfeit production equipment was identified as Member of Parliament, and certain assets traced to a Cypriot holding.

Duration of project: 18 months

Resources employed: 30 investigators; 10 security auditors; three lawyers; two analysts; two accountants; three security consultants; and several teams of bodyguards for the client's senior managers directly linked to the anti-counterfeit operation.

CNS RISK

In Collaboration with Clients' Counsel and Advisors

CNS Risk is an experienced global investigator. We know where to look for 3rd party information that can cast new light and reveal unseen relationships in data already held by the client.

- We ensure chain of custody remains traceable and defendable and that evidence is always accessible for counsel.
- Data gathering is done in accordance with relevant regulations in the given jurisdiction, and can be carried out on-site, at the corporate HQ, or in neutral territory.
- Where investigations span multiple jurisdictions, data can be acquired remotely and stored and processed at a data center of the clients' and/or counsel's choice.

Further Information

For immediate investigation response please contact:

Nicholas Sarvari at nick@cnsrisk.com
Matthew Higginson at matthew.higginson@cnsrisk.com

Request a demo of the CNS Risk Enhanced Investigation Technology Toolset: info@cnsrisk.com

CNS Risk Ltd.
2 High Street, Chobham,
Woking, GU24 8AA
United Kingdom
Office: +44 20 3773 4002
info@cnsrisk.com

CNS Risk Ltd.
1052 Budapest
Vármegye u. 3-5
Hungary
Office: +36 1 411 3602
info@cnsrisk.com