

# Fraud Intelligence

## Into the unknown

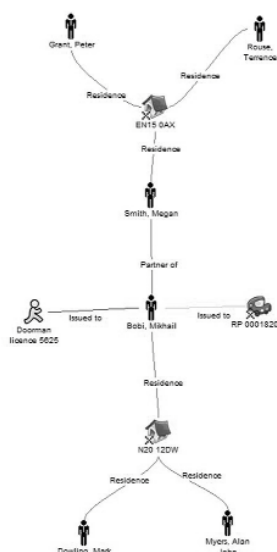
*Multiple targets, assets, objects and thousands of transactions – how are they connected, how can they be? Jane Inzani of ebis Analytics draws out an answer.*

For many years now Government departments' specifications for new IT systems have included a requirement for data visualisation. Agencies involved in investigations – the investigative arm of HM Revenue & Customs, the Police National Database, and a number of systems for Intelligence Agencies – have all included visualisation requirements. Those involved in the prevention and detection of crime have long recognised the value of visualisation; the ubiquitous i2 Analysts Notebook, for example, has been used by police forces across the world for over a decade. However, use of data visualisation by other organisations with statutory responsibility to protect themselves against economic crime and fraud – including banks, mortgage providers and life insurance companies – or those specifically targeted by criminals, notably those who embrace the electronic tools of the modern age, has been extremely limited. This is despite the fact that visualisation technology has delivered documented, unique results and is now relatively mature.

### Degrees of separation

At this point it is probably useful to clarify what is meant by 'link path analysis'. Most of us are familiar with the proposition that every person is linked to every other person in the world by no more than six degrees of separation. Link path analysis applies technology to that concept and visualises the links, not to the whole world of course, but using the information that we hold. Everything is linked in a database. A person will be linked to an address and this address may appear in another table that links it to another person, and so on. Traditionally, to discover this link we would call up the report on the first person, and then request a report on the address. In this simple example we have two separate reports and they hold the knowledge that the first person is linked to the second person by an address. The problem with this approach is that should this exercise go further we end up with a pile of reports and it is down to the keen eye of the reader to spot links across them. In the example

shown [below], the link map reveals that an individual, Mikhail Bobi, is connected to five other people, four of them by a common address. Visualising the information removes the risk of missing the link – if it is in the database it will show up.



Even this uncomplicated use of data visualisation can prove extremely helpful as the case of a viral fraud impacting a credit card company bears out. The company knew which customers had already defrauded but it was unable to work out who would do so next. At the point of applying a data visualisation tool to the data it had some 3,000 separate pages of information – the answer was in there somewhere. By the time we were instructed, several analysts had already been working the case for three months. Application of the visualisation tool to the data took a day, a link to a number of addresses was then found in less than five minutes, and a recurring pattern in company registration forms and directorships after a further 10 minutes. In these circumstances, arguably, visualisation is the only tool for the job.

But such maps are not just useful in fraud detection. They have an increasing role in compliance. Let's take a simple example. It is common to accept utility bills as proof of address and identity. We check the bill, it looks genuine and the application is rubber-stamped. But we

do not check to see if the bill is unique to the application. Interestingly, many schools no longer accept utility bills as proof of address because staff know they are easily obtained to support fraudulent applications for places. However, the time and cost to implement even the simplest of additional checks on an application, whether for a mortgage, credit account or insurance policy, are often viewed as prohibitive, a weakness exploited by the fraudster. Email addresses are often ignored but this is extremely helpful to the criminal, who is able to run all his activities from a single virtual mailbox. Visualisation lends itself to one-off or routine checking for common addresses.

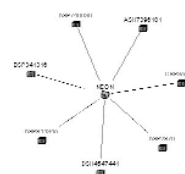
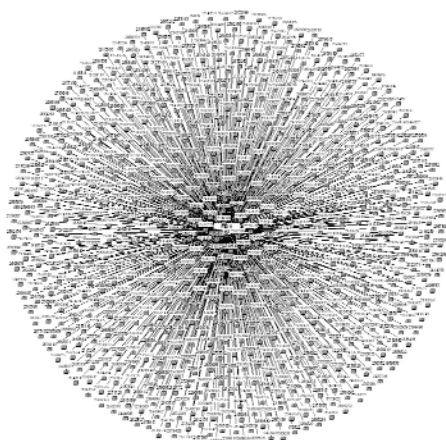
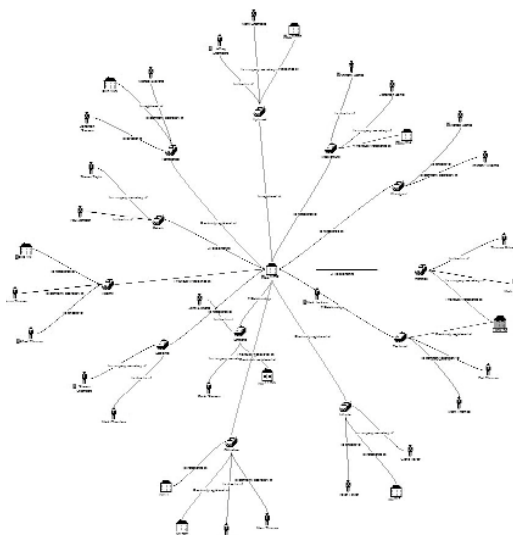
Traditionally, visualisation techniques, as the name suggests, have been used to draw pictures of complex situations. There is an obvious value in revealing connections, and highlighting the key players, be it in fraud, money laundering or terrorist networks, is much easier and more immediate. However, using these tools merely to depict a past event misses their true investigative value.

The earlier example displayed objects – people, addresses and licences – and relationships, the links between them. But much more information on these elements can be included, like date and time, values, text, etc, and these can in turn be used to manipulate the “picture” and test the data. In practice, this means that highly transactional data such as emails or bank account payments can be analysed simply by removing irrelevant information from the picture and focusing in on those data that are important, such as subject or date. Data that was previously too daunting to go through is now in the sights of those who need to know what took place. In Images 2 and 3 (bottom of page), the display of a highly connected

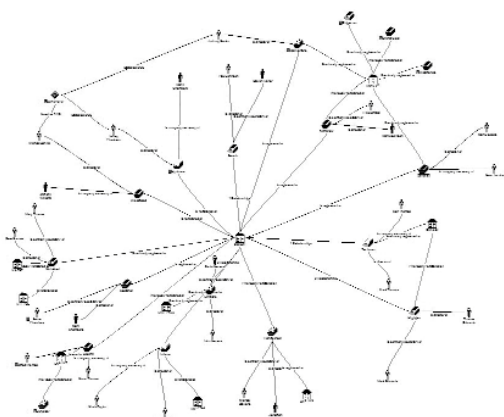
object has been simplified to show only objects that occurred within a specific period. This exercise took seven seconds to complete – complexity of the data set and the connections therein will certainly affect the time but the message is, it is fast.

E-disclosure is an obvious candidate for visualisation. Disclosure often produces masses of information that must remain largely unsearched without the capacity to go through the material, let alone conduct meaningful analysis. In one case a company director was suspected of disclosing confidential customer data to a competitor. The proof was found in one email amongst hundreds of thousands.

Visualisation also lends itself to understanding whether revealed networks are reasonable or suspicious. This is not difficult. Image 4 (below) contains some interesting patterns – each of the end groupings are very similar, which an analyst familiar with the data may or may not expect.



If we expand the network further the objects will develop on routes of their own totally unconnected to each other. One level further and an outer ring starts to appear, linking the objects not just to the central point but also to other common objects (see below). Without visualisation, this evidence of collusion would be virtually undiscoverable. In the hands of a skilled operator, this sort of information can then be used to discover similar networks and suspicious groups.



Such exercises take relatively little time, a network can be displayed in a matter of seconds, making it possible to check literally thousands of objects and connections within days. The process can be learned, the patterns understood and leveraged as fraud teams bring their own experience to bear. In place of sampling, it is now possible to guarantee that every object is examined.

If the advantages are clear, why do so few organisations make use of visualisation tools? One common perception is that it takes a lot of work to prepare data for analysis. However, many tools will work directly on any relational database and consultancies now offer visualisation pre-packaged with popular commercial

databases. Most of the tools also provide a means of ingesting data into a specially designed repository that is both scalable and quick to do – the author has experience of a 30 million object database that took less than a day to ingest. It is also possible to hand load information, which may not be as stupid as it sounds if, for example, you do so whilst reading case notes and papers.

These techniques are easy when applied to relational databases or information that has been structured in some way, such as a spreadsheet. However, many financial institutions possess data stored in forms that have not been converted into a relational database, or unstructured data in reports, letters and emails. Here, too, there are plenty of products on the market, like Captiva and ISIS, that can quickly convert forms and unstructured data into a construct for visualisation. There are also consultancies that will perform the task and, in addition, offer specialised visualisation and analytical experts who understand where the relevant information is likely to be found. The data barriers no longer really exist so it comes down to the will to do it.

Every profitable organisation is an attractive target to those who seek to commit fraud. Criminals act fast and react even more rapidly, as one door closes they are already looking for another still open. Organisations must keep up by deploying tools that are both flexible and smart.

The availability of data visualisation may well, in the eyes of both regulators and stakeholders, raise the bar for what is considered ‘reasonable care’. In these circumstances it is a brave company that does not at least explore its potential.

*Jane Inzani is a director of ebis Analytics Limited (+44 (0) 20 7531 9555, [jane.inzani@ebis.co.uk](mailto:jane.inzani@ebis.co.uk), [www.ebis.co.uk](http://www.ebis.co.uk)). ebis Analytics provide specialist services to financial services companies, the legal sector and fraud professionals, to transform large amounts of complex data into actionable intelligence to assist in the prevention and detection of fraud and economic crime, and exceed the benchmarks for compliance.*

**Editor:** Timon Molloy • Tel: 020 7017 4214 • Fax: 020 7436 8387 • Email: [timon.molloy@informa.com](mailto:timon.molloy@informa.com)

**Editorial board:** John Baker – Director, Business Integrity and Investigation Services, RSM Bentley Jennison • Neill Blundell – Head of Fraud Group, Eversheds • Andrew Durant – Senior Managing Director, FTI Forensic Accounting • Chris Osborne – Director, Dispute Analysis and Forensics, Alvarez & Marsal

**Production Editor:** Frida Fischer • Tel: 020 7017 5501 • Email: [frida.fischer@informa.com](mailto:frida.fischer@informa.com)

**Publisher:** Nic Whyke

**Sales and renewals:** Pauline Seymour • Tel: +44 (0) 20 7017 5063 • Email: [pauline.seymour@informa.com](mailto:pauline.seymour@informa.com)

**Subscription orders and back issues:** Please contact us on 020 7017 5532 or fax 020 7017 4781.

For further information on other finance titles produced by Informa Professional, please phone 020 7017 4108.

**Printed by:** Premier Print Group • This newsletter is printed on paper sourced from sustainable forests.

**ISSN 0953-9239** © 2010 Informa UK Ltd

**Published 6 times a year** by Informa Professional, Telephone House, 69-77 Paul Street, London EC2A 4LQ. Tel 020 7017 4600. Fax 020 7017 4601. [www.informa.com](http://www.informa.com)

**Copyright** While we want you to make the best use of *Fraud Intelligence*, we also need to protect our copyright. We would remind you that copying is illegal.

However, please contact us directly should you have any special requirements.

While all reasonable care has been taken in the preparation of this publication, no liability is accepted by the publishers nor by any of the authors of the contents of the publication, for any loss or damage caused to any person relying on any statement or omission in the publication. All rights reserved; no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electrical, mechanical, photocopying, recording, or otherwise without the prior written permission of the publisher.

**informa**  
law  
an informa business