DIGITAL FOOTPRINTS – THE KEY TO SUCCESSFUL FRAUD INVESTIGATIONS

A growing reservoir of data can now be used by investigators to uncover wrongdoing at an early stage and trap fraudsters before they do significant damage

From the moment they wake up in the morning, almost every human being contributes to their individual digital footprint. As well as our text messages, emails and online searches, we are sharing information about our activities and location with a growing number of organisations.

Now this vast and growing reservoir of data can be used by organisations to do more than just improve relations with their customers and other stakeholders. The digital footprint created by every individual is finding a new use as it enables organisations to investigate fraud more quickly and accurately and to be more confident of convicting wrongdoers.

Digital footprints can facilitate fraud investigations

Whether it is a case of manipulating financial statements, favouring a particular supplier in return for an illegal economic incentive or making dishonest expenses claims, almost every action connected with fraudulent activity will be recorded at various locations in an organisation's IT servers.

As they carry out investigations, organisations' in-house lawyers and external legal advisers can use this digital footprint to expose and ultimately prove wrongdoing. In addition, Big Data and machine learning can be used to investigate it more accurately and in greater detail in order to uncover wrongdoing and reveal cases of identity theft. It can also enable anti-fraud vetting systems to evolve in order to keep abreast of the fraudsters' latest attempts to keep their activities secret and to obscure their digital footprint.

Collating data to provide insights

Finance companies such as Visa and Mastercard, for instance, are already investing in behavioural biometrics. This technology records the ways in which people scroll on screens and read on phones and tablets as well as the angle at which they hold these devices. As part of a user's digital footprint, this information can then be used to alert the relevant authorities when someone other than the authorised user is accessing a bank account or other sensitive financial information. These innovations can be used to identify and investigate cases of internal, as well as external, fraud.

However, vast amounts of raw data are of little use to investigators and legal teams looking to convict wrongdoers. Only when it is analysed accurately and in a timely manner with key patterns and relationships identified, can this data that makes up a person's digital footprint be used to reveal fraud – and to do so before significant losses are incurred.

Since such data is often dispersed across various databases and servers within the organisation, it is essential for investigators that it is coordinated and collated. The fraudster's digital footprint, just like that of any other individual, will, for instance, cover their emails, phone calls, texts, social media posts, payments made and received and even their physical whereabouts.

Data included in downloads, web browsing histories and card swipes can all be used to create a more comprehensive and more accurate profile of a suspected fraudster's activities.

New opportunities emerge but compliance remains essential

Following a digital footprint across multiple sources of information can reveal, for instance, a sudden change in spending patterns by an individual or unexplained increases in payments to certain suppliers or external bank accounts. Even the abrupt increase in interactions with a particular website or the unusual delivery of goods to a hitherto unrecorded customer and location can be used to identify a case of possible fraud by an employee.

Following an individual's digital footprint offers new opportunities for investigators, but they should ensure that in doing so they comply with all data privacy regulations. The increase in data and the ability to analyse it increasingly accurately will evolve over the coming years. Already it offers in-house legal teams and external investigators and advisers the prospect of identifying wrongdoing more quickly while greatly increasing the chances of successfully prosecuting those responsible.

Muthmainur Rahman, senior managing director, head of Middle East forensic technology

FTI CONSULTING

Office 604, Index Tower, Dubai International Financial Centre, United Arab Emirates.

Tel: +971 (0) 58 562 4020 **Email:** MRahman@fticonsulting.com

Web: www.fticonsulting.com