

## The Industrialisation of Identity Fraud – experience of cyber gangs from the UK

*Fuelled by the growth of the Internet, identity fraud has over the last ten years transformed from cottage industry to a mass-market crime opportunity operating on a global scale. Experian Decision Analytics' Fraud Consultancy team explain why the criminals ultimately responsible for the bulk of identity fraud will remain untouchable and how the organisations with most to lose can take the lead in foiling the fraudsters.*

Ten years ago it was a lot more costly to obtain someone's details and, therefore, it was more difficult to make a profit out of identity fraud. Identity frauds were committed by opportunist thieves and small time crooks that had stumbled on an opportunity or had stolen information – in person – from wallets, handbags, homes and dustbins.

While they still represent a threat, dustbins and other personal effects are no longer the data sources of choice for identity fraudsters. Bin raiding is dirty, unpleasant manual work, and any form of direct theft includes a high risk of being caught. In addition, consumers are more aware than ever of the risks of disposing of sensitive information and are increasingly shredding important documents. Dustbins simply are no longer profitable for the serious identity fraudster – who is now e-enabled, IT savvy and (anti-)social networked.

The dramatic increases in identity fraud we have witnessed over the last few years have coincided with its movement from being predominantly opportunistic into the realm of organised crime. While the small-time identity fraudster remains, the bulk of identity fraud today is carried out by no more than a few hundred sophisticated criminal gangs running identity fraud rings involving a complex network of associates, middlemen, techies, hackers and runners, often recruited and managed via the Internet.

These gangs collate and misuse data on a mass scale, creating longer term opportunities and utilising economies of scale to turn large profits that fuel lavish lifestyles and nefarious activities such as drug running and international terrorism.

The onset of the knowledge economy – made possible by the growth of the Internet – means that data is more easily available to identity fraudsters than ever before and has made it possible for them to operate across global borders. Gangs obtain the vast majority of their illicit data via the Internet, often with help from a highly trained 'techie'.

Often engaged as an anonymous freelance resource – recruited online via one or more, middlemen – the techie will hack into a target IT system, or develop trojans, worms and phishing scams to access personal information. This data will be passed back up the chain to the criminal gang where it will be stored on personal PCs or memory sticks. Alternatively, the gangs or their contacts, will obtain the data they require from individuals within the target organisation.

Once the data is obtained, processed and misused, the gangs will then turn to a 'runner', who will act almost as a personal shopper for the criminal gang. Gangs will operate local runners in different markets to do the risky business such as skimming cards, obtaining cash on 'stolen' cards or collecting illegitimately obtained merchandise. Naïve, expendable and operating at the bottom of a long chain, these individuals are the drug mules of the identity fraud world, the easiest to spot and the most likely to be arrested and prosecuted.

To minimise their own chances of being uncovered, the gangs structure their operations in a complex manner, layering their external relationships and utilising the relative anonymity of the Internet to remain remote and unaccountable from other parts of the fraud ring. Even if a runner is pulled in, it is unlikely they will know anything about whom they are working for.

Gangs deliberately operate across international borders. For example, an Italian based gangster might arrange to steal data relevant to US citizens via a techie based in Russia. He could then place postal redirects, divert telephone numbers and add secondary identities to an account, and arrange for cards to be dispatched to UK mail boxes for a UK runner to pick them up and obtain cash and high value goods anywhere in the world.

In which location is the crime committed? Which police force will investigate? Who will prosecute? Are there extradition agreements in place? Even if the gangs were identified, bringing those who are ultimately responsible to justice is a massive jurisdictional nightmare.

Even on a local level, identity fraud is not investigated on the same scale as other types of serious organised crimes. Undercover surveillance operations are expensive and require highly trained experts from the worlds of law enforcement, financial services and information technology to dedicate significant time to collaborate their efforts. Unfortunately, financial crime is not high on the police agenda, despite the recognition that it funds other illicit activities.

In addition, an undercover operation to follow the identity fraud chain necessitates leaving the runners in place while intelligence is gathered to get closer to those ultimately responsible. This, however, leaves the financial organisation open to suffering further immediate financial losses and damage to its reputation, making it an option few are willing to take.

Another recent development in the way the gangs operate is to take the data they have obtained and to store it to misuse a number of years later. There are two motives behind this. Firstly, by holding on to the data it becomes less risky for the fraudster as it is then more difficult to find commonalities between fraud cases and more difficult to spot the cause of the leak. Secondly, the data held may be more valuable in the future.

For example, if an identity fraudster could obtain sensitive data concerning all final year students at a major university, the amount of available credit the fraudster could misuse will be much higher five years down the line once the students are in the world of work and earning decent graduate salaries. At this later stage, it becomes more difficult to spot the common patterns and links – i.e., former student of university X – and much less likely that the source of the data breach can be found and the offender caught.

International borders, confusion over where the crime is committed, the remoteness of the gangs from those at the sharp end and the anonymity of communications over the Internet, make policing identity fraud almost impossible. For every runner the authorities take off the street, there are plenty more desperate individuals willing to take their place, and the gangs continue to operate with impunity.

There are well documented steps being taken to combat the identity fraudsters, and to minimise their impact. Consumer awareness of identity fraud has never been higher and sensible organisations, wide awake to the reputation damage a breach could cause, have taken steps to maximise their data protection systems.

Consumers have recognised the value of shredding their personal data; however, they must also accept additional responsibility to help protect their personal data. Consumers must take more care online and also when answering cold calls, not to give away account details and passwords, and also monitor their credit reports for any unusual activity, by registering for an identity fraud monitoring service.

In addition, organisations have a duty to provide assistance to those consumers who have been affected, and through its free Victims of Fraud support service, Experian leads the industry in helping consumers mend the damage caused by identity fraudsters.

Meanwhile, identity fraud rates continue to rise and, with the authorities unable to get to the roots of the problem, it is up to those that have the most to lose – the financial services sector and the wider credit industry – to act make it uneconomic for the criminals by preventing frauds, not just at the point of application, but throughout the entire lifecycle of an account.

Fraud is a non-competitive issue and all industry sectors need to work together to combat it. Increased data sharing is a must, to allow those organisations being targeted to have the widest possible set of data to find patterns and links to prevent fraudulent applications, compromised accounts and breached data assets.

Finally, more effort needs to be put into fraud awareness training, to ensure that those responsible for preventing fraud at the point of application are up-to-date with the latest fraud trends and developments, and therefore better prepared to combat this growing global problem.