THE changing face OF FRAUD

An extract from Perspective: The Fraud Issue

Essential insights into the issues facing your industry today
The changing face of fraud

In a world where complex algorithms are used to spot online behaviour, and where a continuing set of new gadgets, apps and platforms transform our lives, have the older rules about identifying who we are run their course?

Fundamentally, as the scenario at the start outlined, only a few details are used currently to identify or verify an individual. Typically, these involve addresses, date of birth, mother’s maiden name and/or a combination of passwords or PIN numbers. And, in a world where we have so many details to remember, it is not surprising ultimately, if many people use as few sign in details as possible, or have passwords or PINs that are easy to recall. Add to that the explosion in services available online and social media, and what this means is that the same information that has been used to identify or verify an individual for many years, is now very likely to be easily available online to criminals: whether it is through hacking, use of malicious software, fake websites or trawling through social networks to see what people unwittingly reveal.

Over the past decade, identity fraud has gone from a crime that typically targeted certain types of people (normally professional males in their forties or fifties) to one where people are targeted more indiscriminately, for smaller sums. In 2012, identity crimes (impersonation or the takeover of an existing account) accounted for 66% of all frauds identified by organisations that share data through CIFAS. So, nowadays, it is highly unusual for the modern fraudster to target just one person for a £20,000 loan as they did 10 years ago. Now, they will target 10 people for credit cards of £2,000 each. And, in each case, it is the ease and availability of data that helps the criminal.

Of course, ease and convenience aid the organisation and customer too: so, is it time to ask ourselves whether we need to re-examine – fundamentally – how we do business both as organisations and as consumers? After all, if you asked friends, family or colleagues what details might ‘identify’ you as an individual, they are far more likely to provide details relating to your physical appearance, personality and character than a date of birth and answer to a simple question such as ‘where were you born?’ Recent smartphone advances have involved the use of a ‘fingerprint scanner’, while in some countries, biometric scans such as palm prints or scans of veins in fingers are used to access bank accounts. If details like these are a little too much for some, how do we (as a society) feel about our banks or other service providers knowing a little more about us? After all, many of us – without realising it – receive adverts when we are online which are tailored to us: as our internet browsers and systems keep a note of our online habits.

Organisations make use of advanced data sharing techniques, rules and technologies to prevent fraud, so is it time to start making use of similar techniques in order to prevent fraudulent transactions and applications? Fundamentally, is the convenience that we enjoy actually helping the fraudsters? If so, what can we do to stop it?

For more information, contact Richard at richard.hurley@cifas.org.uk.

¹ To see the full details of the poll, please visit: http://www.cifas.org.uk/fraud_trends_march13.