The true cost of fraud

An extract from Perspective: The Fraud Issue

Essential insights into the issues facing your industry today
The true cost of fraud

Perspective invites John Marsden, Identity & Fraud expert at Equifax, to share his views on the real cost of fraud to consumers, and to organisations like yours.

The cost of fraud to the economy is a hot topic of debate, which is unsurprising; the figures are astounding. It hits everyone’s pocket in one way or another and it often seems that the fraudster is driving the types of cars the majority can only aspire to own. With these challenges it’s clear that, fundamentally, the organisational need – and moral imperative – is to stamp out fraud.

Yet while professional and opportunistic fraudsters appear to be prevalent across numerous industries, there are an equal number of careers being made in preventing these crimes. The fraud ‘arms race’ will continue to show innovation in both the way fraudsters choose to attack and the responses such attacks require.

But let’s reflect a little on our own experience.

Precious time

Typical law-abiding citizens often find themselves facing barriers, such as anti-fraud screens, in the digitisation of their day-to-day lives. This means that the cost of fraud prevention to the consumer amounts to more than pounds and pence: the real cost is the time that we, as individuals, need to invest to prove we are who we say we are.

The inconvenience of taking time out of our valuable lives to get copies certified and sent over to a provider or presenting ourselves at a branch can be a huge pull on our personal resources. Neither the consumer, nor the business requiring these checks, want this ‘friction’ involved in the client on-boarding process. The whole operation can cause delays and, ultimately, client dissatisfaction, lost sales and significant process costs for all parties.

Presenting this with a slightly different twist, it shows that it is not so much the loss of the asset that matters to consumers, (which organisations are often quick to address), as the time that the whole process takes.

Does authentication mean frustration?

The often unexplained, and perhaps seemingly mysterious, phenomenon of identity verification can frustrate and confound the genuine consumer. The documentary process described above is just one example of this friction. Thankfully, the use of electronic data is reducing the need to provide certified copies or actual documents when it comes to proving our identity.

We now enjoy a more digital approach to authentication and identity challenges. Having worked in the industry for many years, I know what is behind the scenes and often understand why I am being challenged, but this may not be the case for everyone else.

The security challenges of knowledge based authentication (challenge and response questions), passwords and picture selections, along with out of band challenges (such as SMS, voice response and email response), are all perfectly valid. They have a place in protecting businesses and consumers from criminals. The question is more about appropriate use. With the coming of useful and usable biometrics, the use of facial and voice authentication might make this a little easier, but I still suspect a large element of society will have difficulties.

The use of fraud intervention techniques needs to take into account all the technical and data aspects available, which – if practiced correctly – should facilitate a frictionless process under the right conditions. Ultimately, the need to provide the consumer with a great experience, while still protecting them and the business, must be at the centre of what we do. We should bring our professional understanding to each client interaction and use the right techniques to challenge clients appropriately.

The challenges of regulation

Money laundering regulation has resulted in a good discipline in counter fraud measures for the regulated sectors. The basic concept of Customer Due Diligence (to comply with Know Your Customer) ensures that a reasonable fraud screen is in place for all regulated companies. Money laundering customer due diligence is often seen as separate to anti-fraud efforts but aligned with anti-fraud technique: it offers a very formulaic approach to anti-fraud. However, a good understanding of the regulation is a great starting point for building anti-fraud strategies.

The AML regime has been successful in ensuring we have a level of knowledge about who our consumers are and that we have some detail to ensure they are who they say they are.

However, the attempts to ease the customer boarding process are often counter intuitive when balancing the client experience against the need to comply with the money laundering directive. For example, the mitigation of impersonation is a legal requirement and the Joint Money Laundering Steering Group (JMLSG) guidance notes go so far as to explain a number of ways to do this (JMLSG Pt1 5.3.83). This can be achieved through various processes but some do cause friction. This needs careful consideration because if one individual business adopts a measure that is likely to cause friction for the consumer, they may lose business to an organisation that doesn’t. None of these businesses want to support or suffer from fraud, they simply need to be aligned with their industry to be in business.

My personal nirvana is for organisations to know who I am as a consumer, understand my good standing and facilitate the simplest of journeys through the customer boarding process.

The world of adaptive authentication is a science and its analytical approach is borne from the individual’s need to move through the world unhindered, supported by electronic interaction. Just because we can challenge and create hurdles to access services does not mean that we should.

This is reflected in the results of a CIFAS poll which showed more than 41% of people felt that the ‘time lost trying to clear up the mess’ was the worst side effect of being a victim of fraud.¹
In an ideal world, we should remove those hurdles for those who are shown to be genuine customers, and the secret to achieving this is in the data and the technology.

The not-so-old paradigm of putting people through the same process regardless of trends, silent identification methods and normal practices, is being removed, reducing friction for the consumer. Based on solid data, science and technology, the reason for a business to invest in this is simple: customer experience = customer loyalty. I am not unique in wanting attempted frauds to be challenged but, at the same time, I do not wish to be subjected to those challenges in my normal life. Technology truly enables this, in this regard. Those businesses that do not adapt will suffer client dissatisfaction and loss of business.

Getting it right

Let’s look at two systems that are common and accepted ways of reducing fraud: ‘Verified by Visa’ and ‘MasterCard Securecode’. The implementation of these systems – known collectively as 3Dsecure – was absolutely necessary for banks to facilitate a controlling function over the challenges when the Visa/MasterCard was not presented at the checkout (Card Not Present – CNP).

It is widely accepted that cardholders generally disliked the imposition of an additional box at the checkout. Shopping basket ‘drop-out’ was a major issue for retailers throughout the implementation of 3Dsecure and subsequently many retailers pulled out either before or shortly after implementing the check. Having another few clicks at the checkout, even when the consumer knew their password, created friction in their experience. And while the password reset function on 3Dsecure is relatively easy and designed to help the consumer to finish their shopping, checkout abandonment remained an issue. Let’s face it, if I order a weekly shop from the same retailer with the same delivery address, same card and the same electronic device, do I really need to authenticate? This relies so heavily on observing the transactional traits, the device and the data that this has been difficult to implement due to the lack of great technology to decide on the levels of risk presented by a transaction.

One particular technology company has been deployed to do just this within 3Dsecure by a card issuer. I love it: it facilitates, saves me time and ultimately does not deter from my purpose. This card is my preferred payment mechanism for internet purchases and remains ‘front of wallet’ in my purchasing choice. The operational challenge is being able to spot these trends, devices and transactional details. Once these are secured, we can rest assured that suspicious transactions are challenged accordingly (with friction) and non-suspicious transactions go smoothly.

Equifax has data, analytics and technology that enable an organisation to respond according to the situation presented by the consumer.

Once again, I understand why I am being challenged when I change PC, Tablet or phone – and would expect to be challenged. Elements of the fraud community do recognise these techniques and there is never a silver bullet, but through progressive authentication we can stay fresh, current and secure. All in all, the majority of people are not fraudsters and deserve to interact with financial institutions and retailers with a certain degree of measured trust. We are entering the world of progressive authentication and we are applying vast resources in order to enable people who have nothing to hide to enjoy a superior customer experience with the organisations they choose to interact with.

The future of fraud prevention

There will always be instances of a genuine customer being challenged out of band, given that two-factor or knowledge based authentication are the current ‘flavours’ of challenge. However, biometrics is the new frontier in an adaptive or progressive authentication product and this is on the near horizon. I do love to see this working because, when it works correctly, my normal life is facilitated.

My final thoughts turn to my mother, who phones me every time she gets a phishing email or when she gets challenged by knowledge based authentication or out of band challenges such as SMS or email. Often she ends the call reassured, whilst I end the call worried, but that’s just a mother and son living in very different times. Using our approach, my mother’s service provider (bank or card company, for example) would be informed about the risks of an interaction, enriched in their response and empowered to react in the right way. Ultimately, this means less friction for all of us.

The way technology facilitates my life is truly amazing and the dynamic work of making my navigation through the electronic interactions of every day is truly empowering. I am proud to be part of this revolution. Let’s talk about how we make people’s lives better and ensure that we continue to challenge where risk is demonstrated.

For more information please contact John at john.marsden@equifax.com or on 07789 996557.

¹ CIFAS Victims of Fraud press release, 22 March 2012.