Fraud's new mobile playground

Mitigating risk and defending consumer threats under the changing landscape of customer engagement.

Introduction

In just a few short years, the world of identity, personal and financial fraud has come a long way since the proliferation of card skimming, identity theft from documents and fraudulently obtaining a PIN over someone's shoulder.

The criminal network behind fraud is a sophisticated, agile and clever one; as soon as a new way of illegally obtaining personal details for financial gain emerges, the information spreads like wildfire and crimes are very quickly committed.

Newer communications channels are naturally the most exposed in the early stages of adoption, for a few reasons. Firstly, for many technology companies, the need to be seen as forward-thinking, cutting edge and ahead of the curve in terms of meeting the modern consumer's need to be connected anywhere and at any time, can often outweigh the need to put in necessary precautions, preventions and fail safes against the misuse of the data that is being sent and received via these devices.

Secondly, it stands to reason that regulatory frameworks need to mature through increasingly widespread use of new technologies and channels. Applying the same rules that govern technology such as online banking through a web browser means that vulnerabilities can be exposed quickly, and fraudsters will always find a way in.

Thirdly, and perhaps the most critically, there is an inherent nervousness surrounding new technologies in terms of whether it's going to generate robust revenue streams for manufacturers and service providers, that can often be the catalyst for a lack of investment into security and ultimately, the prevention of fraudulent activity.

With smart technology, led by the mass adoption of smart phones, tablets and other internet-connected devices, security issues are still being researched and understood, especially given the rate at we are seeing 'smart' being attached to everything from televisions, cars and games consoles, to refrigerators, energy meters, and even the simple light bulb. The buzzword of the day is 'The Internet of Things'.

Connectivity truly is the new lifeblood of our daily lives today, and it shows no sign of slowing.

Gartner predicts that 4.9 billion connected 'things' will be in use in 2015, while IDC says that there will be 28 billion by 2020. These estimates have been backed by industry plans, with a recent statement from Samsung Electronics' CEO Boo-Keun Yoon claiming that 100 per cent of the company's products will be connected to the Internet by 2020. These 'things' have their own IP addresses; they're already getting smart enough to capture data from sensors and process it in a way that can be delivered in an understandable way to the consumer in order to generate meaningful, and contextual 'intelligence' from which decisions can be made. Naturally, as adoption matures and prices come down, the 'hub' of this information, which will display it in a digestible way, will be our smart phones and tablets – our mobile 'life support'.

Internet of Me

Before prices dip enough to take us past the early adopter stage and into the majority, context is critical to making the IoT work, making our lives easier so that we find that like many people with a smartphone, we cannot live without it. It also has to be profitable in business; otherwise there would be little impetus for companies to manufacture IoT objects beyond a reputational boost among industry commentators and customers. Therefore those in the market of IoT are looking to ingratiate relevance into the technology. This is about making those connections both meaningful and contextual to the end user.

For a customer interaction to be meaningful, it also has to be personal to them. To be personal, forget guesswork – information on that person must be used, wherever that may be gathered from. Every time a sensor reads data or a person inputs into a device, whether that is walking, breathing, talking, or even typing in a credit card number – this data is being recorded and stored in the cloud. Less The Internet of Things – increasingly so, The Internet of Me – and individuals and organisations with fraudulent intentions want to hack us.

Fraud follows the channel of adoption. As we adopt more and more connected objects, fraudulent activity will attempt to follow – and often succeed.

A fraudster's playground

The phenomenal volumes of data already flowing through the information ecosystem – whether that's a traditional network or the cloud – represents a touch point ripe for fraud. Every time we will input some data – whether manually or automatically via sensors – we are interacting with an organisation of some type, meaning that there is a huge onus on banking institutions, the mobile network

operators, and telecoms companies, as well as operating system providers, to enable the right levels of protection.

It is not just the consumer market at risk however; a Business Insider survey into industry adoption trends of the IoT, speaking to technology executives in early 2015, found that the biggest barrier to investing in the IoT is "concerns about the privacy and security aspects", with almost 2 in 10 (39 per cent) of the sample identifying this. From the experts to the everyday person – it's plausibly easy to fail to be aware of the implications of inputting personal data when users are given the impression of high security, with long sign up processes, identification procedures and possibly even multi-factor authentication methods for every log-in.

The more touch points, the more channels that connect the Internet of Me to companies, the more opportunities there are for fraudulent activity. The more of your personal data – including credit card and bank account details, lifestyle data, geographical data and so on – that leaves your fingertips or sensors within IoT objects and goes into the connected world, the greater the risk of these details being misused by people.

The October 2014 Crime Survey for England and Wales found that in the region, there was a rise of 8 per cent year on year in the volume of all types of fraud, though the CSEW claimed that this was a difficult figure to measure accurately, since the figure is based on public reports to the Police and other institutions, such as the banks. It suggests that the actual levels of fraud are "severely under-reported".

Smart, internet-connected, mobile fraud needs to be tackled from the ground roots up by providers and banks; after all, the smartphone that will live in the pockets of more than half of the world's population by 2017, according to Forrester . And when it comes to the data we're increasingly sending across the networks? According to a large consumer study across 22 countries in late 2014 by Bain and Company , banking interactions are now happening through smartphones and tablets more than any other channel. In fact – mobile accounts for around a third (30 per cent) of the total number of banking interactions worldwide. Combine this with a recent report from mobile payments company Zapp , which found that 44 per cent of consumers would be prepared to switch banks if their current bank was unable to offer mobile payments and had no plans to do so, and the demand for increasingly being able to manage all aspects of a person's life from their smart device, is clear.

This is about as attractive as it gets for a fraudster, and there are a number of ways in which cyber (or mobile) criminals are obtaining identities and private data. Unfortunately, mobile is a gaping hole in an otherwise well-established firewall of IT security solutions that are far more sophisticated than ever.

Contextual security

The first key challenge is that traditional IT security is like putting a square peg in a round hole when it comes to mobile; it doesn't work and leaves vulnerabilities.

While adware, malware, Trojan-style attacks and now 'man-in-the-app' threats are easier to get onto more modern mobile devices because they are increasingly being made to run several applications at once. Some IT security providers have issued mobile versions of their popular anti-virus desktop programmes, but there are several more sophisticated and lesser known – yet growing in volume – ways in which a person's details can be captured and misused.

In 2014, awareness around the growth of phishing attempts grew with threats such as Cryptolocker and Gameover Zeus – both of which can use malware and other programmes to access personal details when accessed on mobile devices. The fact that typically 'desktop computer' threats could now affect us wherever we are came as a surprise to many banks and telecoms companies, as fast fixes and patches were developed to quickly put consumers' minds at ease. The threats could also take advantage of holes in 'weaker' customer engagement channels such as SMS and mobile web apps, leaving payment and banking apps open to abuse.

Other more silent, but deadly threats came from the likes of SIM Swap; whereby someone unlawfully obtains a duplicate SIM card for a mobile number – using the same method as someone who has genuinely lost their SIM or mobile device – and fundamentally re-directs communications back to the fraudster. A victim is unlikely to discover the incident for days, meaning that criminals are able to access anything linked to that number – including any synced public cloud accounts or data held on the SIM card itself – such as one-time passcodes.

In the same way traditional anti-virus or anti-malware programmes work, responding to these threats after the fact, and having static security in place, is no longer effective with the mobile/internet-connected device channel. Banks and telecoms providers need to be proactive.

Gartner recommends that organisations begin the transition to context-aware and adaptive security infrastructure now, rather than sit and respond to threats after they've occurred. What the latter can potentially result in is angry and frustrated customers and a damaged reputation, not to mention a difficult clean-up operation. A lackadaisical attitude to preventing mobile fraud in the first place, in a proactive manner, will result in happier and safer customers, as well as protection for an organisation's own investments.

The second challenge is the user experience. Customer engagement processes need to be adequately secure, yet do not compromise the freedom to move between contact channels, or the expected 'ease of doing business' with the bank, or a retailer, public sector service – any transaction for which personal or financial data crosses the network. Using a multi-factor or multi-layered approach to securing data is an increasingly favoured method by banks, but it still needs to be perceived as easy and fast by the user, without disruption to their day. One-time passwords, for example, are a resilient method of authentication, but often the delivery of these to the customer can be disrupted by network traffic, and if the vulnerable SMS channel sends these, there is a significant risk of fraudulent interception if SIM Cards are swapped.

Banks therefore face a significant challenge in a competitive market; are they seen as a reactive organisation with the bare minimum of security measures in place in favour of a smooth user experience via mobile devices, or do they implement tougher controls that require users to take part in long registration or log-

in/authentication processes, yet risk customers getting frustrated and moving to a competitor that doesn't?

There is an inherent need to make the priority awareness; alerting people and banks to the threat of these viruses will go a long way in making customers aware of the dangers and how to protect themselves, and in turn helping to develop the technology that perfectly combines ease of access with protection. However it may be a case of both customers and banks deciding what's more important to them, which will not be an easy decision to make.

The role of data, big and small

Banks and telecoms providers have a significant role to play in the fight against fraud. The wealth of analytical data obtained from the connected devices is one of the greatest strides towards being able to effectively and accurately ascertain new risks, and monitor this new threat landscape. With all eyes on the headway retail banking has made in performing online and mobile transactions, it stands as a perfect example of how so-called 'Big Data' can improve resistance to fraudulent activity while banking online, and at the same time significantly improving the customer experience.

There are currently A multitude of ways in which the mass of data generated by mobile devices can be used to proactively detect fraudulent activity, prevent misuse, and secure personal data, all without compromising on the user experience. Through collaboration, banks and telecoms providers can take up the context-aware, proactive mantel to better focus resources where they are needed more – on the customer experience, and not losing money through tidying up crimes once they've occurred. Banks can instil customer trust and confidence in their services, and telecoms providers can ensure a smooth user experience for their tariff holders.

- *Divert detection*

  Real-time checks that can be performed at the telecommunications level when a call is made, to verify whether outbound calls have been diverted to another telephone number, via mobile or landline. These checks are completely transparent to the user. Contact centre operations can use this method as a layer of verification of outbound calls, to ensure that they are speaking to the correct person. If fraudulent activity is detected, automated communication can be triggered

- *SIM Swap detection*

  SIM Swap detection transparently establishes whether a customer's SIM card has been duplicated using mobile network data. A person with an unknown compromised SIM card would be at very high risk of fraudulent activity, enough to even access a bank account from the device; detected SIM Swaps can be identified as genuine swaps (e.g. a new phone), or suspicious, and bank access/mobile network access suspended pending further investigation

- *Location-based services and proximity*

  These preventative measures take into account the geographic location of the mobile device by harbouring location data to draw conclusions as to whether activity is lawful or not. Location can be used in relation to known fraud hotspots, and establishing historical patterns of mistrust. Proximity looks at the location of the mobile device in relation to that particular transaction or action being conducted. For example, if a mobile payment was being made from a different country to where the device was, there is a high risk that it is a fraudulent transaction

Aspect works with banks and telecoms providers globally to optimise every facet of customer engagement, including deploying sophisticated fraud detection and multi-factor authentication methods. Aspect Verify, a solution suite of anti-fraud services and part of the Aspect Proactive Engagement Suite (PES), is specifically designed to meet the challenges of the digital, mobile world. Aspect Verify prevents fraud through increased security utilising mobile devices, and improves the proactive detection of fraud, so customers ultimately feel more confident making digital transactions.

1 http://www.gartner.com/newsroom/id/2905717
2 http://www.idc.com/downloads/idc_market_in_a_minute_iot_infographic.pdf
3 http://www.cloudpro.co.uk/cloud-essentials/4742/samsung-commits-to-open-internet-of-things
4 http://uk.businessinsider.com/internet-of-things-survey-and-statistics-2015-1
5 http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-june-2014/stb-crime-stats--year-ending-june-2014.html
6 https://www.forrester.com/Forrester+Research+World+Mobile+And+Smartphone+Adoption+Forecast+2014+To+2019+Global/fulltext/-/E-RES118252
7 http://www.finextra.com/news/fullstory.aspx?newsitemid=26840
8 http://www.finextra.com/news/fullstory.aspx?newsitemid=26836

Corporate Headquarters East
300 Apollo Drive
Chelmsford, MA 01824
+(1) 978 250 7900 office
+(1) 978 244 7410 fax

Corporate Headquarters West
2325 E. Camelback Road,
Suite 700
Phoenix, AZ 85016
+(1) 602 282 1500 office
+(1) 602 956 2294 fax

Europe & Africa Headquarters
2 The Square, Stockley Park
Uxbridge
Middlesex UB11 1AD
+(44) 20 8589 1000 office
+(44) 20 8589 1001 fax

Asia Pacific & Middle East Headquarters
8 Cross Street
25-01/02 PWC Building
Singapore 048424
+(65) 6590 0388 office
+(65) 6324 1003 fax

About Aspect
Aspect is the only software company with a fully-integrated interaction and workforce optimisation platform for enterprise contact centres globally that need to profitably (and seamlessly) orchestrate people, processes and touch points in an era when the contact centre is the new centre of the customer experience. For more information, visit **uk.aspect.com**.