BLECKWEN

AUTHORISED PUSH PAYMENT FRAUD:

The perfect storm that devastates lives

BLECKWEN

AUTHORISED PUSH PAYMENT FRAUD:

The perfect storm that devastates lives

Contents

Introduction	2
Part One: The anatomy of APP	3
Part Two: The storm clouds gather	5
Part Three: What can be done?	8
About Bleckwen	10

www.bleckwen.ai | **contact@bleckwen.ai**

Immeuble Belvédère,
1-7 cours Valmy,
92800 Puteaux,
FRANCE

BLECKWEN

AUTHORISED PUSH PAYMENT FRAUD:

The perfect storm that devastates lives

The Digital Revolution is changing our lives every day, but human nature does not change, and with every technological advance, new crimes emerge. As digital makes deeper inroads into our financial affairs, we are all increasingly exposed to fraud. Most of us will have had a transaction blocked because our bank suspected that it might be fraudulent. In 9 cases of 10, banks have been overzealous, and the payment is eventually cleared.

Financial institutions are right to err on the side of caution, but it comes at a cost as every (false) alert has to be actioned. For the customer, the experience of having a bona fide transaction blocked for no apparent good reason is nothing but frustrating. It is reassuring to know that in the case of actual card fraud, the customer is protected. Usually, the amounts of money involved are relatively small — an average of just over £250 in the UK — and any loss incurred is reimbursed by the banks. Card fraud is growing, but not as fast as another type of fraud where the average loss is considerably higher — more than £4,000 – and which is not generally reimbursed. Authorised Push Payment (APP) Fraud, as it is called, is attractive to criminals for two reasons: the sums stolen are much larger, and banks have on the whole been helpless in detecting and preventing this type of fraud attack.

APP Fraud is particularly abhorrent because its victims are often - although by no means always - vulnerable and elderly.

In this white paper, we analyse the drivers and effects of this insidious type of fraud, but more importantly, what banks and financial institutions can do to combat it. Before we move on to describe what APP Fraud is, and what damage it does, a brief note about some of the perceptions, and misperceptions, about its victims. APP Fraud is particularly abhorrent because its victims are often - although by no means always - vulnerable and elderly. This segment of the population tends to be more inexperienced about the pitfalls of social engineering than most other age groups. They are also richer, having accumulated wealth in pension schemes or in their homes, where equity release provides rich pickings for the criminals.

However, anyone can be a victim of APP Fraud. A recent case that made the headlines in the UK was that of a former BBC sports presenter who was scammed out of £70,000 by a fraudster "impersonating" her bank[1]. "It was just a few questions," the 36-year-old commented. She went on to say: "It [APP Fraud] happens every day of the week. We're not talking about little old ladies who don't understand the internet, that's a massively naive assumption. It's happening to people and they're too embarrassed to say that it's happened." What makes these stories especially heart-rending is that victims of APP Fraud are left out in the cold because they have no legal redress and generally do not get their money back, as we shall see.
The moral outrage engendered by this state of affairs is ratcheting up the pressure on politicians and financial institutions to act.

1 - Ruby, J. (2019) BBC host Helen Skelton reveals she was scammed out of her £70,000 life savings.

BLECKWEN

PART ONE:

The anatomy of APP

The rise of Faster Payments networks and growing customer expectations of a smooth if not friction-free banking experience is creating the ideal conditions for APP Fraud.

In an Authorised Push Payment scam, a criminal tricks his victims into sending money directly from their bank account to an account controlled by the scammer. In essence, this is a human hack that bypasses the controls and cyber defences put in place by banks and financial institutions, because it looks — or it appears — no different from the hundreds of other transactions a customer may make each month. The fact that banks are not usually able to detect these scams explains why criminals are ramping up their APP activity. There used to be little statistical information around social engineering and APP Fraud, but gradually we are gathering more granular data.

In the UK[2], one of the few countries to track this emergent fraud in detail, £354m was lost through APP scams in 2018, a rise of 50% on the previous year. The number of reported cases almost doubled and reached 84,624 in 2018. Not only is APP Fraud becoming more prevalent, it is also accounting for a larger share of the money stolen through all types of banking fraud. In 2017, APP Fraud represented just under 24% of all fraud; this crept up to 30% a year later. But as Faster Payments becomes more deeply embedded in our lives, and the default method of transaction processing throughout the world, APP crime is expected to increase at an exponential pace.

£354m

lost through APP scams in 2018 (UK).

84,624

reported cases of APP fraud in 2018 (UK).

2 - All the UK figures in this paper come from the report UK Finance – Fraud the facts 2019. Available at: https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019

How do APP fraudsters perpetrate their crimes?

The use of social engineering tactics through deception and impersonation is a key driver of APP scams. Typically, this involves the criminal posing as a genuine individual or organisation and contacting the victim by telephone, or via email and text message. Criminals also use social media to approach victims, with adverts for goods and investments that never materialise once the payment has been made. The moment the victim has authorised the payment and the money arrives in the criminal's account, the criminal will quickly transfer the money out to numerous other accounts, sometimes abroad, where it is then cashed out. This can make it difficult for banks to trace the stolen money.

There are a number of APP scams and these continue to evolve as criminals refine their approach or devise new ways to deceive their victims and the banks. However, they broadly fall into the following two categories.

i. Malicious Payee: This first category involves Purchase scams (by far the largest of APP scams), investment scams, romance scams (just 2% of APP Fraud) and advance-fee scams, which predominantly target consumers.

ii. Malicious Redirection: The second category targets both business and consumers. Malicious Redirection is broken down into invoice and mandate scams including; CEO fraud, impersonation of police/ bank staff (as in the case of the BBC presenter) and a scam known as "other impersonation".

Malicious Payee accounts for 78% of all reported cases of APP Fraud, but only 35% by value as the average fraud event is comparatively small at £1,900. Malicious Redirection accounts for just 22% of cases but 65% by value with an average event value of £12,000. **How do the criminals get away with it?**

30%
of total fraud
(2018 UK).

£4187
average event
(2018 UK).

50%
growth
(versus 2017 UK).

BLECKWEN

PART TWO:

The storm clouds gather

Over the decades, banks and financial institutions have built a maze of controls and cyber defences to combat fraud, funding for terrorist activity and money-laundering. The rules alerting a bank to (possible) fraudulent activity are usually rather broad, resulting in transactions that are perfectly above board being blocked. As we saw, this is a source of constant irritation to the customer - but blunt rule-based systems are also a headache for banks who have to verify each alert.

With APP Fraud, the robustness of a bank's rules-based defences is almost irrelevant, because the "criminal" transaction coming in looks like a perfectly ordinary transfer from a customer who interacts with the bank many times a week to pay for shopping, book a holiday, order goods online, put money in a tracker fund and so on. The fraudulent transaction is initiated by the customer on his or her usual device, and very possibly through a banking app that sent the customer a security code, which was duly typed in - and so the payment went through.

In effect, the individual customer is a Trojan horse that slips the criminal through a bank's cyber defences and controls. When the fraud is detected, the enemy is already within the gates. This is what makes APP Fraud so dangerous for banks - it renders traditional defences almost powerless.

Of course, banks do train their staff to look out for tell-tale signs of APP Fraud but for criminals, there is an easy way around that: digital banking. In the UK, 90% of APP Fraud is committed on digital channels.

Additionally, 93% of fraudulently obtained transfers are sent over a Faster Payments network so the banks have little time to intervene and prevent the criminal from moving the funds. In 4% of cases, the proceeds of fraud are moved abroad to make it even harder to recover the funds for reimbursement.

90%

of APP Fraud in UK is committed on digital channels.

93%

of fraudulent transfers are sent over a Fast Payments Network.

"The individual customer is a Trojan horse that slips the criminal through a bank's cyber defences and controls.

The APP Fraud epidemic

We have been using UK statistics because Faster Payments networks (where APP Fraud thrives) have been common in the United Kingdom for several years. As Faster Payments becomes globally established through international networks such as SWIFT gpi, APP Fraud is expected to soar and take on epidemic proportions. At the same time, it is unlikely that existing fraud detection and prevention systems will be capable of detecting worldwide APP Fraud for the many reasons we outlined above.

When technology or regulation changes, criminals devise new ways to exploit that technology or circumvent the regulation. Take the example of the US, which has witnessed a big shift towards CNP (Card not present) Fraud since it introduced EMV - the technology for fast payment using Europay, Mastercard and Visa - in 2015. As it is easier for criminals to circumvent EMV than to produce false credit cards, counterfeit fraud became much less prevalent.

Australia has recently introduced a new national Faster Payments network and as you would expect, APP Fraud is on the rise. During the first half of 2017, Australian companies were the world's second most popular target for business email enterprise (BEC) scams such as CEO fraud. Australia received over 27% of global BEC attacks[3], trailing only the US. If the UK is a leading indicator, this will get a whole lot worse. The real tsunami will occur when the US finally implements Real-Time Payments (RTP) - and all the evidence points to the complicated and heterogeneous US banking system not being prepared for that.

The damage done by APP Fraud

Victims of APP Fraud are as unwitting - and as innocent - as victims of card fraud, but that is not how current legislation looks at it. As noted earlier, victims of card fraud are protected and are reimbursed, whereas money lost through APP Fraud is (usually) money lost forever, with the sums involved considerably much higher.

Regulators and banks are trying to remedy the situation with contingent reimbursement schemes but these are voluntary. Of Malicious Payee scams, a paltry 8% of total funds stolen is reimbursed. (The figures vary from scam to scam with romance scams coming out worst, with reimbursement in just 5% of cases.) The picture is somewhat better for Malicious Redirection, with a reimbursement rate of 31% across the different categories. Overall, just 23% of money stolen through APP Fraud finds its way back to its rightful owner. Incidentally, in 2017, this figure stood at 26%, so the gap we are describing between protection against card and APP Fraud is actually widening.

77%

of victims will not get their money back.

3- Australian Cyber Security Center Threat Report. (2017) https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf

BLECKWEN

The damage done by APP Fraud

Digging a little deeper, we find that 93% of APP cases affect consumers and that between them they represent 64% of all APP losses. As it affects consumers, APP Fraud costs an average of £2,900 per case, and only 19% of total losses are reimbursed. Remember, this does not mean that victims recoup 19% of the money taken from them - some will get more than that, but most will get nothing at all.

This is nothing short of scandalous, but UK financial institutions have been woefully inadequate in their response, with TSB the honourable exception.

Research has shown that nearly two-thirds of households would struggle with an unexpected bill of over £500, so a hit of nearly 6 times that amount from APP Fraud would have a life-changing impact on people with the financial disarray potentially driving many into expensive debt arrangements or destroying life savings (as happened in the case of the BBC presenter).

Although instances of APP Fraud targeting business are less common, the average loss is much higher at £12,000 - a sum that would lead to serious cash-flow problems for many smaller businesses.

Lawmakers and regulators are under pressure to change the legislation which seems so patently unfair to victims of APP Fraud. This will happen one day. However, in the meantime, banks and financial institutions cannot be seen to be doing nothing - especially as there is now a proven methodology to stop criminals from committing this particularly heinous type of fraud.

£2,900

the average cost of consumer targeted APP Fraud per case (2018 - UK).

£12,000

the average cost of business targeted APP Fraud per case (2018 - UK).

Nearly two-thirds of households would struggle with an unexpected bill of over £500, so a hit of nearly 6 times that amount from APP Fraud would have a life-changing impact.

BLECKWEN

PART THREE:

What can be done?

Banks have tended to respond to APP Fraud by adjusting their rules-based system. This has typically led to a drop in the value of APP Fraud cases - a Pyrrhic victory, as the number of cases tended to rise in response.

The real problem remains that banks have until now not been able to keep an eye on individual behaviours in real-time - the arena for almost all APP Fraud. But this ultimate segmentation of customer behaviour is now within reach. Rapid advances in Artificial Intelligence (AI) are perfecting a technique known as behavioural analytics to detect payment anomalies which the fraudster may have tricked their victims into making.

Unlike rules-based systems which treat bank clients as part of a much larger segment (i.e. consumers or small businesses), AI can track hundreds of variables in real-time at the individual account level to spot specific anomalies for each account and each client, and flag these to a fraud expert – in real-time 24*7*365, regardless of the channel being used. So, as more clients turn to digital and ever more digital channels to make payments, all these channels can be simultaneously monitored for APP and other types of fraud, such as account takeover and internal fraud.

The real problem remains that banks have until now not been able to keep an eye on individual behaviours in real-time - the arena for almost all APP Fraud.

Metaphors do not prove anything, yet it is tempting to put it like this: traditional APP Fraud detection consists of looking out of the window to see if it is raining, but behavioural analytics is a barometer.

It gives banks a channel and payment-type-agnostic view of fraud for each individual client in real-time, around the clock, greatly enhancing its security - at a lower cost to the bank (not to mention the savings that flow from preventing instances of fraud, and the reputational damage that inflicts).

There is more. If behavioural analytics did not adapt to change it would not be much good, because this is what behaviour does - it changes. AI, as it were, becomes one with an individual account holder's payment profile and adapts as that person's transactional behaviour changes, which he or she is bound to do as new payment types and methods become available. AI also learns from feedback on what is fraud and what it is not, as analysts interact with the system when they process alerts, making the system smarter over time which means it will create far fewer false positives.

Where Explainable AI is used, the amount of client friction and the time needed to resolve a fraud alert go down because explainability guides the fraud analysts to focus on the most prominent things out of the hundreds of possible variables that triggered the alert. This reduces the total cost of managing fraud and keeps client friction to a minimum – a win/win for client and bank – and an effective threat response to the ever-changing fraud risk.

If you want to find out more about Explainable AI and how behavioural analytics can protect a bank and its clients from becoming victims of APP Fraud, then please contact us contact@bleckwen.ai

BLECKWEN

About Bleckwen

Bleckwen: the real-time Machine Learning solution for financial crime detection and prevention.

Adversarial by nature, fraud is constantly evolving and requires financial institutions to be ever more vigilant. We address the inadequacy of legacy rules-based systems that cannot adapt to the increasing need for real-time payments and changing customer behaviours. In partnership with banks and financial institutions, Bleckwen combines behavioural analytics with AI to provide effective and robust protection against financial crime. Bleckwen's solution helps teams to focus on what is important, to reduce false positives, customer friction and costs of financial crime detection. Our white-box approach enables banks to reduce the time it takes to process alerts and to comply with increasingly stringent regulatory requirements.

Bleckwen is a French fintech created in 2016. Our models are already used by two French banks. Bleckwen was awarded EBA Fintech of the year 2019.

www.bleckwen.ai | contact@bleckwen.ai |  **bleckwen_ai |**  **bleckwen**