Optal
a wex company

Pushing Back on Payments Fraud

How technology can counter rising risk in push payments

How technology can counter rising risk in push payments

Financial fraud is far from a trend. Rather, it's a constant. Fraud has been ever present since people started buying and selling, and has evolved to become a problem that businesses have to manage and counter every day. Digital evolution has compounded the issue. The areas fraudsters can operate in have broadened and the losses likewise. And, as a financial centre for every business, payments are naturally at the centre of the fraud storm.

Cheque, credit card and cash fraud have all hit hard over the years. However, one of the most common fraud vectors today (and greatest vulnerabilities) is push payments. Particularly for businesses that have relationships with a lot of suppliers, to whom they make numerous payments totalling different amounts all year round.

UK Finance began collecting data on authorised push payments (or APP) fraud in 2017. It recorded losses totalling £354.3 million in 2018, up from £236 million a year before; and 84,624 cases of APP fraud in 2018, a rise of 93% from 2017's 43,875. Businesses shouldn't need further proof that APPs are being targeted. And those that are affected by this kind of fraud generally struggle to reconcile and recover their losses, which can take place across a number of accounts.

So, what can businesses do to avoid it happening in the first place? Arguably, the fightback should not be a matter of protecting push payments, but of using data, automation and insight to have more control over payments.

This is why many businesses are turning to virtual account numbers (VANs) to pay their suppliers – reducing fraud risk, while also lessening their reliance on cheques and BACS over the long term.

Push payment fraud in 2018 rose by 93% on 2017 levels. Making it the fastest growing type of fraud in the UK.

Source: **UK Finance, Fraud the Facts 2019**

The Pull of Push Payments

While push payments fraud mostly affects personal bank accounts, a staggering £126 million hit businesses in 2018. And due to the relatively small size of each fraudulent transaction, it's only the exceptional cases that make the headlines.

A new opt in scheme has been set up to help out consumers who've been the victim of financial crime. But no such scheme exists in the B2B world, which is where things get tricky for buyers whose supplier payments are the target of push payment fraud.

Bad news for B2B

Currently, the responsibility to make good on a B2B payment that didn't make it to the supplier rests with the buyer. Even in cases where an employee mistakenly (but honestly) puts in the wrong bank account details. And while some banks may help out and refund the payment out of goodwill, there's absolutely no requirement for them to do so.

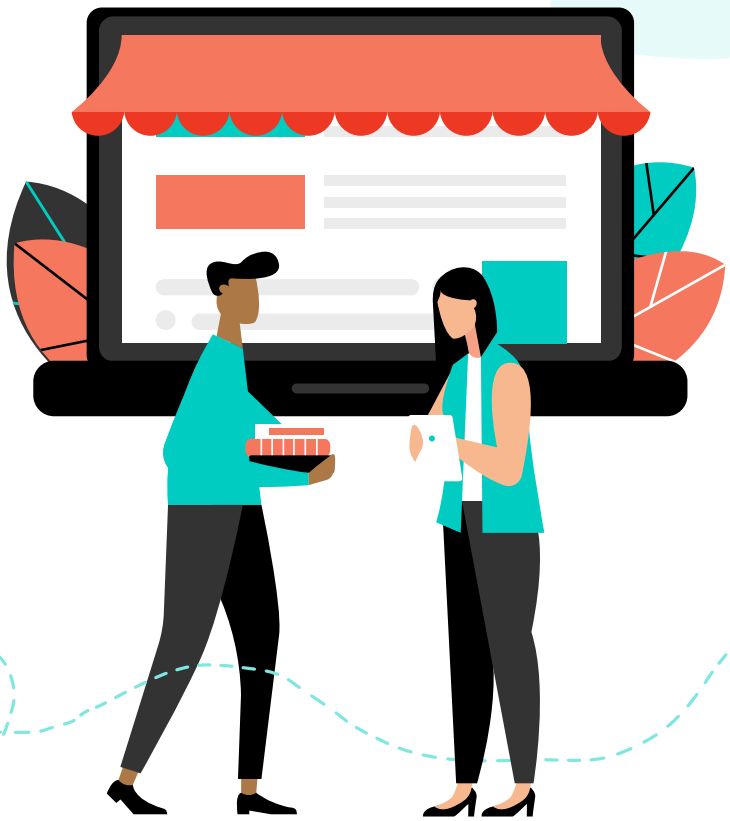
And this is why push is such a pull for fraudsters. Compared to bigger, more notable and newsworthy types of fraud, push payments is a world that's easy to operate in, easy to make money in, and where there tends not to be many repercussions.

It's not hard to see why push payments are on the rise, and why B2B payments are hugely vulnerable (perhaps more so now, given the action being taken in the consumer world). An added challenge is that the staff resources required to adequately prevent, tackle and resolve push payment fraud can be prohibitive for some, with trained IT experts needed elsewhere. These businesses therefore have to find alternative ways to avoid push fraud.

It pays to know your supplier.

Although there are systems to bring new suppliers on board, things can go awry before and after then…

- Unknown Fraud: many businesses won't know that their payment has been fraudulently made until the late payment for an invoice has been investigated, so it can take months before anyone becomes aware that something has happened.



Accumulation of Marginal Losses

When most people think of fraud, they tend to think of big money losses. But push payment fraud is rarely like that, particularly in B2B.

With fraudsters aware that businesses will have a close eye on their big suppliers, they'll instead target the mid-tier relationships. To the fraudster, this makes sense:

- Many businesses will make infrequent payments to their mid-tier suppliers, so there's no regular monthly amount going out, and unlikely to be a common payments pattern
- Mid-tier payments are generally not as large as those made to top-tier suppliers
- Most businesses need a good business case to remediate fraud. If it will cost £300 and significant staff resource to resolve a £500 loss, they probably won't do it

This combination is perfect for push payment fraudsters. But for businesses it can be extremely problematic.

Money, reputation and time

Even though individual instances of fraud may not look huge, put them together and there's a sizeable dent to the bottom line. To the point that some businesses will incur thousands of pounds worth of fraud losses, made up of hundreds of separate incidents.

This on top of the damage fraud can do to a business' reputation if it keeps happening (particularly relevant in industries like insurance, where the payment might be to a facility that's rehabilitating a client after an accident). Not to mention the hours lost to fraud investigation, when staff in finance departments could spend their time better elsewhere.

With payments fraud not going away, and its impact widespread, many businesses are now looking at ways that technology can negate it, removing the vector that criminals attack. The way they're doing this is through innovation – transforming the way they pay suppliers, at the same time as introducing more automation and insight into their payments processes. And they're looking at how technology can quickly address payment problems. Card scheme chargeback rights, for example, allow pull payments to be recalled if sent to the wrong account – helping businesses in the moment.

Payments problems.

It's not just fraud that's causing businesses issues in supplier payments. Misdirection, duplication and late payments are all pain points. A recent survey discovered that around £3 million collectively is misdirected annually. New payment methods like virtual account numbers can help businesses with each of these, as well as protecting against fraud.

Source: Optal, Optimising Payments

Protected Payments, Secure Suppliers

Over the past few years there's been a general recognition from many businesses that established payment methods are not fit for purpose.

Cheques, as many will testify, were a 17th century invention, and are hard to manage in a 21st century financial world for a number of reasons. Business credit and debit cards are useful, but certainly not appropriate for all payment types. BACS, meanwhile, is where push payment fraud is massively on the rise, creating unnecessary cost and risk for the buyer.

Clearly, an alternative is needed. And there are a few attributes any new payments solution will need to have, alongside security.

Model modern payments

Increasingly, there's a need for business payments to be fast, transparent and easy to audit and control as well as secure. It's partly for these reasons that many leaders at the top of banking and finance are looking to virtual account number solutions to both meet the requirements of 21st century finance, and to avoid the push payment fraud risk that's become so prevalent with BACS. Indeed, in their analysis of virtual account management, Accenture wrote that it will 'grow in importance in the immediate future and will definitely be high on the agenda with leading European transaction banks.'

In the world of payments, virtual account numbers are an obvious solution to counter fraud because they, as pull payments, close the door to push-specialist fraudsters. They also don't require payers/buyers to hold the depth of supplier data that push payments require (e.g. bank account details). And because they automate elements of the payments process, virtual account numbers eliminate manual errors and lower the risk attached to payments. There's no need for bank account maintenance, for example. And if something does go amiss, card scheme chargeback rights can allow pull payments to be recalled.

Meanwhile, on the insight side, the inherent transparency of virtual account numbers means it's easy for businesses to see when a payment request was issued, when it was settled and if anything happened in between. This not only makes fraud easier to recognise, but also helps with other time-consuming payments problems that drain staff resource.

Many early adopting businesses have used virtual account numbers for some supplier payments, proving their benefit and creating clear use cases that convince other suppliers to follow suit. In doing so, they're gradually reducing the need for cheques and BACS.

As with many other areas of finance, innovation is providing new ways of countering existing and long outstanding problems, helping businesses fight back against this latest fraud trend.

The benefit of using technology to keep payments safe doesn't stop with avoiding fraud. Businesses who take this route also benefit from better supplier relationships, a revenue boost, and real-time insight into payments processes.

Andrew Downes,
Optal

The Payments Alternative

Businesses with a large amount of supplier relationships face a unique set of problems. They're dealing with a lot of business relationships at once, and generally lack the scrutiny to really understand all of them as much as they'd like. At the same time, the mix of these suppliers is likely evolving and changing, with regular on and off boarding. And on top of it all, fraudsters are targeting the payments they're making to suppliers, knowing that they can make big gains pretty quickly.

It's not a state of play that can feasibly last much longer. So the case for a new way to pay is becoming stronger all the time.

This is why forward thinking businesses are looking to the technology companies that are changing payments with innovation, automation, risk mitigation and data. In doing so, these businesses are not only reducing the risk of fraud, they're also making payments operations smarter, faster, and – in some cases – a genuine profit centre for the business.

In the process they're realising that a new way to pay has the potential to change the role of payments in their business altogether.

If you want to learn more about how to change the way you pay, download our new eGuide about payments alternatives.

To talk to us about how we could add value to your organisation, please contact:
info@optal.com

Optal
a WEX company

Optimise with us

in partnership with mastercard

optal.com

The products and services offered by the Optal group are for exclusive use in business to business transactions and are not available to consumers or the general public (nor micro-enterprises or charities as defined in the Payment Services Regulations 2017).

*All Optal's statistics quoted relate to our 2018 B2B payments report. In cooperation with Mastercard, we asked 100 senior finance executives within FTSE 350 companies and large public sector organisations what they thought of the state of B2B payments. These are their insightful views.