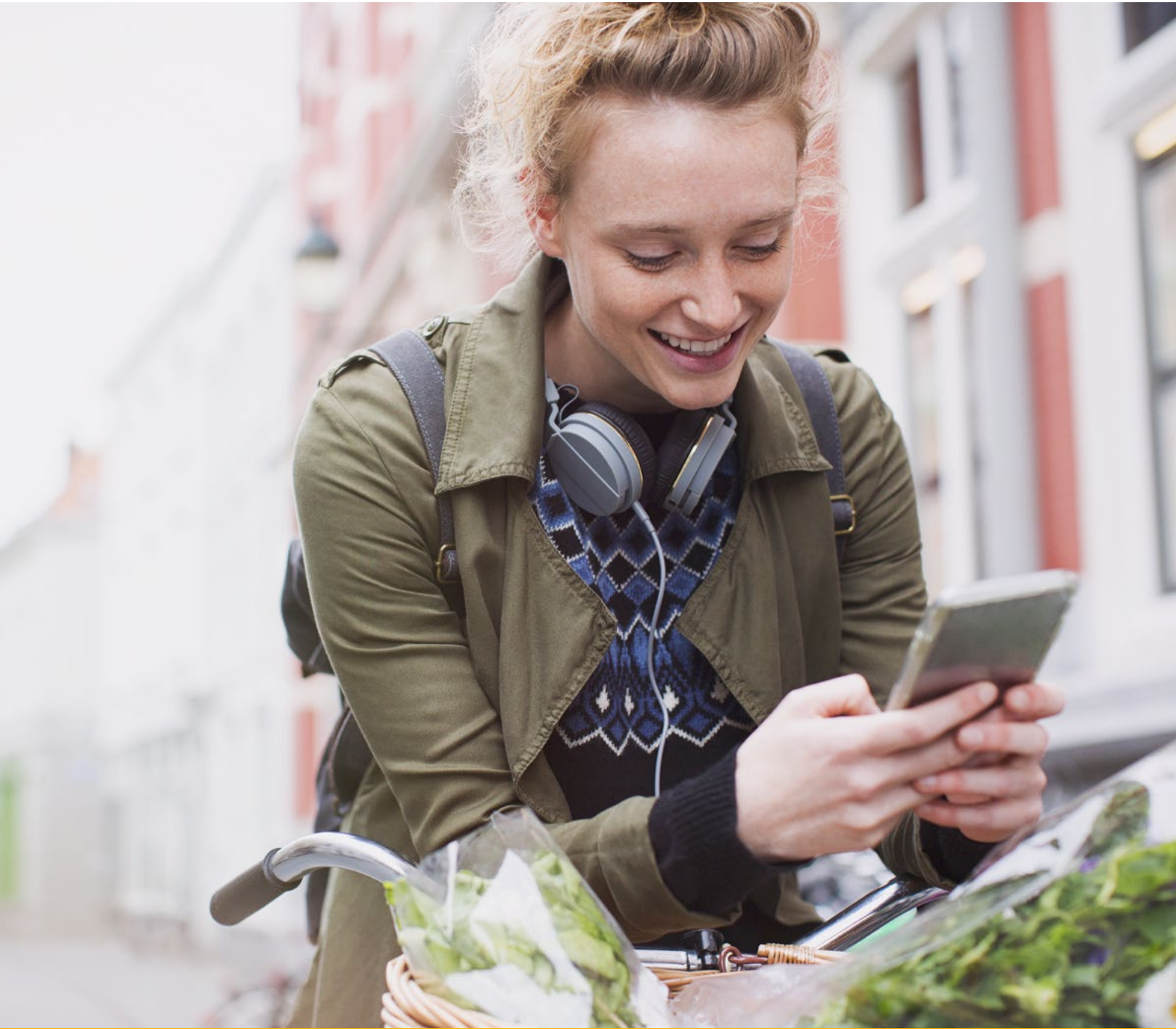


Managing risk. Meeting expectations.

Building a fraud strategy for the digital economy



Agile businesses need agile fraud management

Digital technology is creating change at a pace never seen before. Customers now expect speed, ease, choice and a personalised service.

It makes customer experience key to success. And it sets merchants a challenge. To survive, and thrive, businesses need to stay agile in everything they do – including how they manage fraud.

As the people who set the strategy that determines if an order is accepted or not, fraud teams have a pivotal role to play in improving customer experience and reducing risk. This makes fraud management more than a back-office utility. It's a way to differentiate your business and achieve a competitive advantage.

So, how should fraud teams balance growth and risk in a fast-changing landscape?

This is the question we put to three specialists from CyberSource – as well as Chris Monk from digital literacy agency Decoded.

This report reflects their expert opinion, and explores:

- The changing landscape for businesses.
- The key challenges for fraud teams.
- How to develop an agile fraud solution.



Meet the experts



Andrew
Naumann

Vice President,
Product Management,
CyberSource

“

Andrew has been solving complex fraud issues for two decades. He's responsible for the vision of CyberSource's fraud and payment security solutions and makes sure they always reflect the "merchant view".



Carl
Tucker

Head of Managed
Risk Services,
CyberSource

“

Carl brings strategy, data and technology together to tackle the problem of fraud. He's worked with enterprises in new markets, start-ups, internet brands and more. Through the solutions he builds, he's helping to shape the future of fraud management.



James
Hunt

Senior Director,
Managed Risk Services,
EMEA, CyberSource

“

James is on the front line of fraud management. His team of analysts protects the fortunes of numerous clients in diverse sectors. This gives him a deep knowledge of the challenges fraud teams are facing.



Chris
Monk

Head of Region (APAC),
Decoded

“

On a typical day, Chris might hack in to a (made-up) bank or get a group of novices to code an app. And it's all in the name of demystifying technology. Both educator and entrepreneur, he is a well-known speaker on cybersecurity and commerce.

A changing landscape

“ Buy online, pick up in store. Wearable payment devices. The endless aisle, where digital channels complement and extend the physical in-store experience. They’re all part of the quest to achieve integrated commerce.

Andrew Naumann

Andrew Naumann is explaining the challenge for merchants today. He continues.

“These new models feed consumers’ belief that they should get things quicker and more simply. And if a merchant can’t deliver, people will go elsewhere.”

But keeping up with new models is not the only problem. Wherever there are new ways to do business, fraudsters take an interest. They’re early adopters. And if they can discern a weakness, they’ll take advantage.

Andrew paints a picture: *“Let’s take the buy-online-and-collect-in-store model as an example of something we’ll see a lot more of in the future. You place an order right outside a store on any number of mobile devices. You may not have to give a shipping address. A few minutes later, you stroll inside and collect what you’ve bought.”*

“But fraudsters have latched onto the fact that there’s no time for manual review. There’s minimal interaction. And you know the merchant has to fulfil the order. These factors mean that for a fraudster, there’s a lot to like, which is why down the line, we’ll see it happening more and more.”

Similarly, the freedom to purchase from any device in any geography makes it easier for fraudsters to blend into the background.

Andrew: *“You can even start an order in one place and finish it elsewhere on a different device. It’s all part of the integrated experience today’s consumer demands. And it makes spotting fraud really hard.”*

This all puts pressure on the fraud team to put in place strategies and quickly respond to any fraud patterns – even if they’ve never seen the pattern before.

The challenge for fraud managers is complex but not impossible to overcome. It requires a sophisticated approach that balances customer experience, accurate fraud detection and operational efficiency.

To achieve it, you need to be able to adapt your fraud strategy in the face of a changing landscape. In other words, agility is key.



“ Consumers are in the power position, as 2017 is a golden age of choice [and] convenience.¹

PwC Total Retail report, 2017

¹ PwC – 10 retailer investments for an uncertain future, 2017, p. 2. Available at <https://www.pwc.com/gx/en/industries/assets/total-retail-2017.pdf>



“ The fraud pattern you see today isn't going to be the fraud pattern you see tomorrow.

Carl Tucker

Fraud is changing too:

Chris Monk educates people about threats, such as fraud, for a living. Interestingly, when describing the new generation of fraudster, he chooses to start with what hasn't changed. *"The fraudster's MO remains the same as ever: obtain an ID; then use it to transact."*

Where he sees changes are in the speed and volume of fraud. *"The difference digital tools have made are the scale of information now available; and the reduction in time it takes to obtain (sometimes thousands of) IDs."*

The result is fraud on an industrial scale. And it's prompted fraudsters to get organised. *"Cybercriminals operate like pseudo-companies. They have staff on a payroll. They construct botnets to extend their reach. And they market what they've stolen on the dark web."*

This is another symptom of a digital age: the commoditisation of fraud. It can even be carried out to order – in so-called Attacks as a Service. It seems fraudsters, too, know how to develop new business models to attract their customers.

In 2017,

54%

of shoppers surveyed in the UK said they'd used click and collect in the last 12 months.²

² F. Briggs, *YouGov survey reveals retail customer dissatisfaction at all-time high*, 2017. Available at <http://www.retailtimes.co.uk/yougov-survey-reveals-retail-customer-dissatisfaction-time-high/>

What's driving the pace of change?

Behind the developments in eCommerce is the quest for growth. It's what drives merchants to look across borders and to deploy new channels or technology. But just as commerce evolves, so does fraud.

In a digital economy, fraud teams need to know how they can support growth for the business. Andrew puts it this way: *"The big question is no longer 'How can I make sure that I prevent fraud?' Instead, it's, 'How can I accept as many orders as possible without exposing my business to unnecessary risk or disrupting the customer experience?'"*

Here we look at some of the key shifts merchants are facing, and what this means for fraud management.





“ Account takeover is one of the most insidious forms of fraud.

Andrew Naumann

Account on file – creating a seamless checkout

“Customers want immediate outcomes, which means, ‘I want it now.’” James Hunt gets straight to the heart of the growth in account on file – where merchants store customers’ details so they don’t have to re-enter them every time they buy something. The psychology is, *“I want my card to be on file. So, you know who I am. And boom, I’m ready to go.”*

The problem? *“Suddenly, you’re setting up a whole new fraud vector. No longer are you just evaluating transaction fraud. You’ve got to check that the person logging in is actually the account holder. You’ve also got to look out for people setting up fraudulent accounts using stolen data.”*

Miss this type of fraud and it can do serious harm to your reputation as well as your bottom line. Customers are trusting you with their personal and card data. Fail to protect it and you’ll lose their long-term custom, and potentially that of the people they talk to as well.

“There’s a real conflict here,” James Hunt points out. *“On the one hand, if your account is on file, you can make a one-click purchase and the whole experience is seamless. Even the payment and the other back-office functions happen behind the scenes. But while that’s good news for the customer, it’s also good news for the fraudster. If they can hack a customer’s account, they can make a fast purchase that looks legitimate.”*

Account takeover is an attractive option for a fraudster. And there are more and more accounts to hack. So, it’s not surprising that account takeover is among the top three types of fraud that respondents to our North America fraud benchmark report are most concerned about.³

But despite this threat, only 39% of businesses surveyed had tools in place to monitor account takeover fraud.⁴

For Andrew, account takeover is a clear example of the need for an end-to-end fraud strategy: *“This is a strategy that starts with account creation and takes in every step up to payment. A key pillar is account monitoring. This means you identify a customer every time they log in or change anything about their account – no matter what device they use to interact with you.”*

Customers expect you to safeguard their data. So, account monitoring helps to preserve the customer loyalty you’ve worked hard to earn.


³ CyberSource, *Online Fraud Benchmark Report, North America Edition*, 2017, p.4. Available at: https://www.cybersource.com/content/dam/cybersource/2017_Fraud_Benchmark_Report.pdf. ⁴ Ibid.

The rise and rise of mobile payments

Mobile devices dominate the total minutes we spend online.⁵ So, it's little surprise that mCommerce is growing.⁶

Carl Tucker positions this as an opportunity for merchants – but one that comes with an inherent challenge.

"With a smartphone in nearly everyone's pocket, there are far fewer barriers between someone intending to buy and someone buying. All it takes is a number of taps, which is great news for merchants. But assessing a mobile transaction for fraud is very different to assessing an eCommerce or traditional PC-based order for fraud. The behaviours are different. The data elements are different. The security pieces are different."

A photograph of a woman with long brown hair, wearing a dark jacket, looking upwards with a thoughtful expression. She is holding a white smartphone in her right hand. In the background, there is a large, out-of-focus flight information board with yellow text on a dark background.

Forecasts for Europe's EU 5 show mCommerce will account for 43.8% of eCommerce sales by 2020, compared to 32.9% in 2016.⁷

Merchants intuitively know that mobile demands its own set of rules. That's why they invest so much time, money and resources in building apps and mobile-friendly websites.

And yet some merchants still take the fraud rules that they've used for a completely different channel and try to use them as part of their mobile fraud strategy. Carl gives this warning: *"If these differences aren't anticipated and planned for, organisations may experience higher rates of fraud in the mobile channel than they would like. Or they may reject or review too many genuine transactions. Or both. And as mCommerce is forecast to grow, this could have a progressively worse impact on revenue."*

If you do find your business experiencing an increase in mobile fraud rates – as new business models are introduced – it's important to resist the urge to review or reject too many of your mobile orders. If you respond with rules that are too restrictive, there's a strong chance genuine orders will get caught in the net and be rejected. This would clearly work against your business's need to deliver optimal customer experiences. It can be better in the short term to err on the side of acceptance and work fast to spot new chargeback patterns. Then, quickly develop mobile-specific rules that help distinguish genuine from fraudulent purchasing behaviour, without sacrificing the customer experience.

⁵ J. Karaian, *The mobile internet is the internet*. Quartz, 2017. Available at: <https://qz.com/1116469/we-now-spend-70-of-time-online-on-our-phones/>

⁶ P. Breuer & P. Sjötil, *Doubling your company's growth in a volatile region*. McKinsey & Company. Available at: <https://www.mckinsey.com/industries/retail/our-insights/doubling-your-companys-growth-in-a-volatile-region>

⁷ eMarketer, *Worldwide Retail Ecommerce Sales Will Reach \$1.915 Trillion This Year*, 2016. Available at: <https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-trillion-This-Year/1014369>

Selling across borders

Cross-border sales offer another avenue for growth in the digital economy. And merchants are taking advantage. James Hunt: *"In our fraud report, 76% of UK companies said that they plan to accept orders from new markets in the next year.⁸ Supported by globalisation, new product entries and M&A activity, companies are seeking out opportunities in other countries."*

In terms of fraud, cross-border commerce is a step into the unknown for many of these companies. And, as James points out, *"Fraud thrives when it's under the radar."* It's unsurprising, then, that 62% of UK companies serving foreign markets experience higher fraud rates on cross-border orders.⁹

Just as you need separate rules for different sales channels, you should establish new rules for each region you sell in. The maturity of the local eCommerce market, local laws and regulations, and a myriad of other factors can affect both the level of fraud and how it is perpetrated.

Andrew: *"The truth is the stakes are often higher with cross-border orders. Low authorisation rates and high fees can increase the cost per transaction. At the same time, customers' payment experience could dictate how they view – and talk about – your brand."*

A new geographic market is another example of where it might pay in the short term to accept a slightly higher fraud rate than you would like. Once you've built a bank of data – with the right software and insight – you can monitor fraud levels and begin to help minimise fraud.

If you plan to expand into other countries, it's a good idea to partner with a company that understands the nuances in fraud prevention across regions – and how to react to future potential fraud patterns.

In this fast-moving landscape, fraud teams are acutely aware of the need to develop systems that keep their businesses both competitive and secure. And while there's no one-size-fits-all strategy, there are key principles that merchants can adhere to.

The complexity of the task for fraud teams is clear. They must spot and thwart fraudsters who are using ever more sophisticated techniques. At the same time, they must enable the business to accept as many payment methods as possible and as quickly as possible. Keeping check of how fraud is changing even as the business adapts is essential.

As James Hunt comments, *"The days of creating personas to understand fraudsters are long gone. What we have to do now is understand how a real customer behaves. Years ago, we used to log onto the internet when we got home; now people are on there all the time. If we can analyse a customer journey 7am to 12pm and find out what sets a real customer apart from a fraudster, that information will be invaluable."*

Carl agrees: *"The key to combating fraud is data,"* he explains. *"The more data you have, the more accurate your results. You can train your fraud models, increasing the likelihood of recognising situations you've encountered before. Then, you can block or accept them as appropriate. Data richness plays a key role – it's all about collecting the data points: device type; fingerprinting; IP; geolocation; and other validation services."*

Despite the value of these data sources, a CyberSource fraud survey showed merchants routinely fail to use them. Only 22% of respondents used social networking sites and only 18% used device fingerprinting.¹⁰

Andrew: *"Don't forget, information you know about your customers and the actual outcome of past transactions provide powerful inputs to better identify legitimate or fraudulent transactions."*

\$630 bn

forecasted value of B2C cross-border eCommerce by 2022.

A **120%** rise on 2017.

Forrester Online Cross-Border Retail Forecast.¹¹

⁸ CyberSource, *The Balancing Act, 2016 UK eCommerce Fraud Report*, 2016, p. 30. Available at: https://ctmfile.com/assets/ugc/documents/FRA_2016_UK_eCommerce_Fraud_Report.pdf ⁹ Ibid, p. 31. ¹⁰ Ibid, p. 25.

¹¹ Forrester Data Report, *Online Cross-Border Retail Forecast, 2017 To 2022 (Global)*, April 2017. Available at: <https://www.forrester.com/report/Forrester+Data+Online+CrossBorder+Retail+Forecast+2017+To+2022+Global/-/E-RES137898>

A flexible approach for a digital economy

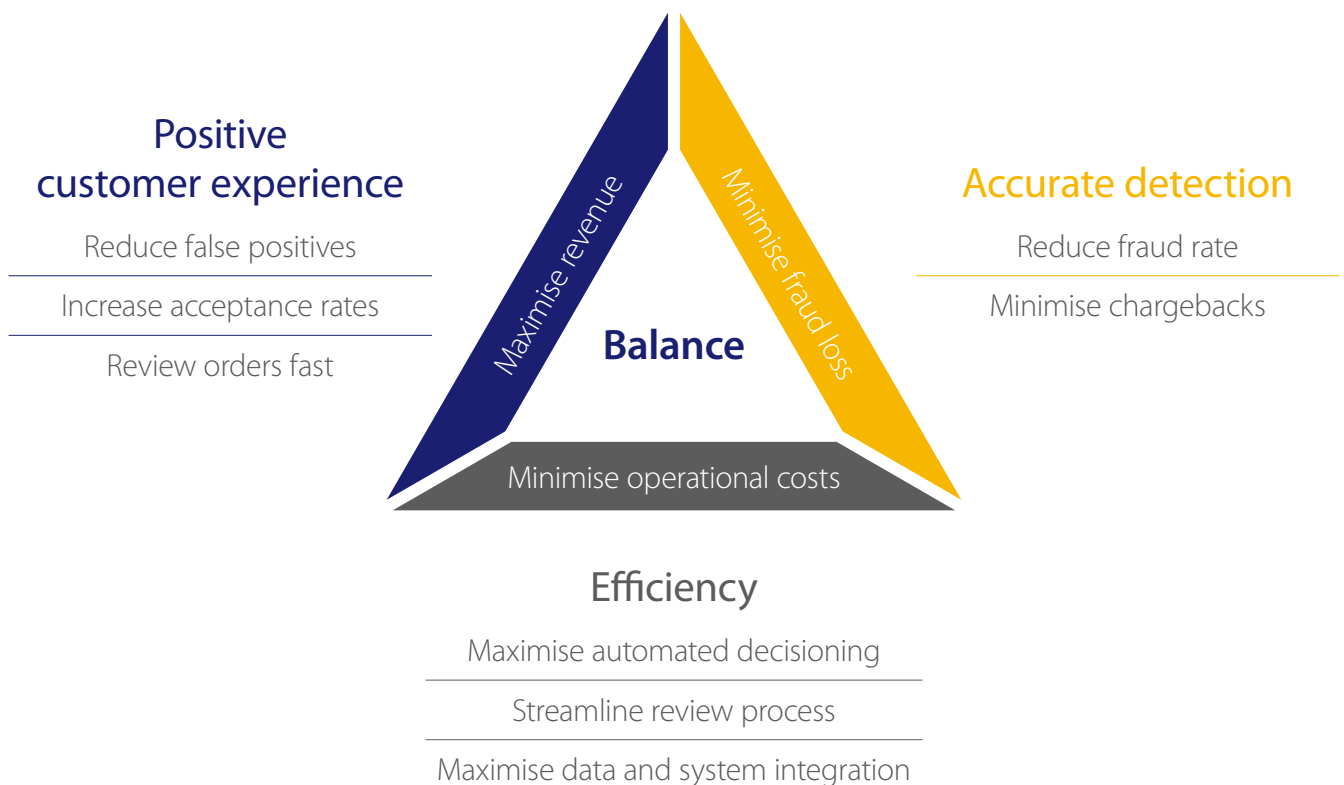
Your ability to support growth depends on finding the perfect balance between three forces: customer experience (CX); fraud detection; and operational efficiency. CX revolves around accepting as many good customer orders as possible and making it quick and easy for people to pay you. This feeds directly into how much revenue you can generate. At the same time, you have to keep fraud in check – to reduce chargebacks. The third thing you have to factor into this equation is the money you're spending to manage fraud. Are you over-reliant on expensive measures like manual checks? Andrew warns that, *"The hard work of generating profit can be undone by operational costs that run too high."*

“ Tiny changes to your approach to fraud can have a huge impact on your bottom line.

Carl Tucker

Diagram 1

Balancing multiple merchant objectives



It's a complex task. Especially in a fast-paced digital market where success depends on being agile. If you throw too many resources at one vector – or skew your fraud strategies in favour of one vector – you can lose out.

For example, a 0.001% fraud rate may sound impressive. But with a figure that low, the chances are that you're rejecting too many legitimate orders. These false positives represent missed profit opportunities for you – and gained revenue for your competition.

By contrast, fraud teams who can keep the three in perfect harmony are set to optimise profits. The aim is to find the profit optimisation point – as shown in the graph below.

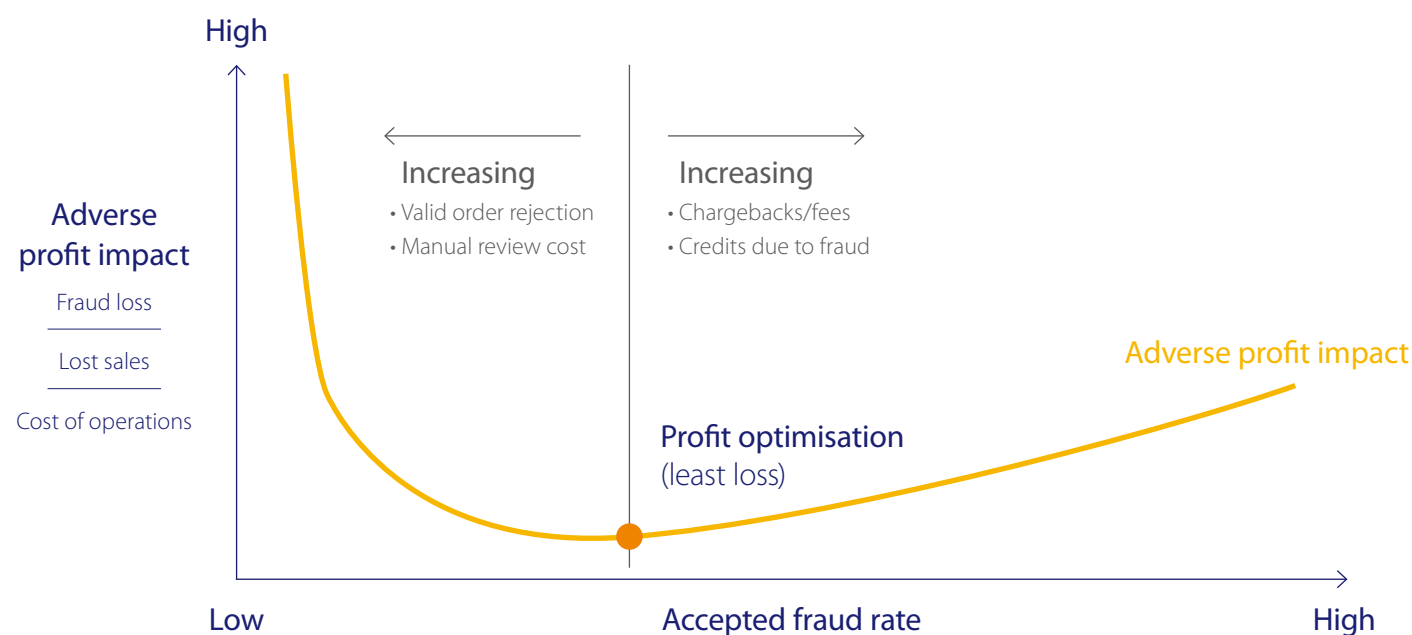
You need to pull all the right levers to optimise profitability. Getting both an ideal fraud rate and an ideal acceptance rate takes a holistic view. Andrew: *"The digital economy requires a multi-phased approach to fraud management. One that begins by reducing the threat of fraud when the customer first establishes an account, and continues all the way through to the moment an online transaction is approved."*

So what approach should fraud teams take to help them manage risk and optimise profits? Next, let's look at how you can continue to tackle fraud in a fast-changing digital landscape.

Diagram 2

Goal

Profit optimisation



Picking an agile fraud management solution

Merchants are encountering new channels, new markets and new challenges as a matter of course. For this reason, you need a fraud solution that is as agile as it is powerful. Below, we explore the main capabilities you should look for.



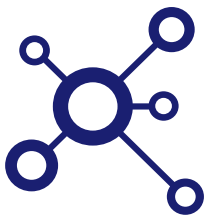
1 Secure account creation

Managing fraud needs an end-to-end approach. This means that your fraud management solution needs to be able to identify fraud – and genuine customers – when accounts are created and every time someone logs in. It must then continue to monitor accounts for suspicious behaviour.



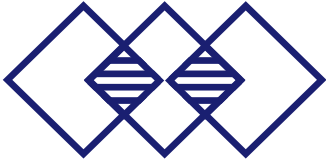
2 Multiple machine learning techniques

New fraud trends are emerging all the time. To respond, you need to combine: the proven effectiveness of conventional static models; and the more agile data analysis of today's most advanced self-learning models.



3 A large global data set

The more data available, the more accurate the machine learning models will be —and the faster they can get up to speed. So, look for a fraud solution that draws on a large external network of merchant data and risk indicators. Whilst at the same time being able to incorporate data from your business.



4 A customisable rule engine

To adapt and stay agile, a flexible rules engine is needed to customise rules and models to your specific business across all sales channels. It also needs to enable swift and accurate responses to unique or emerging fraud trends, at any time; and clearly show what rules were triggered in a decision.



5 Real time analysis

To optimise your fraud management strategies, you need to know how well they are working. You need ways to test “what-if” scenarios with existing fraud rules and see strategy results now; rather than waiting several months to receive chargeback information.



“ At CyberSource, we draw on insights from more than 68 billion worldwide transactions processed annually by Visa and CyberSource. And we use a flexible rules-based engine, called Decision Manager. It uses more than 260 anomaly detectors and 15 region, channel and industry-specific risk models, each tuned to identify fraud in different scenarios.

Carl Tucker

Conclusion

Managing fraud. Maintaining the customer experience.

In the digital economy, fraud teams have an opportunity to make a real difference to the resilience and growth of their businesses.

It follows that fraud teams should be involved in the development of new payment experiences. They are central to the viability of new channels and markets. As such, they have a role far beyond back-office processing and need to be included in conversations about meeting customer expectations.

If fraud teams are to respond to the demands of the business, they have to be agile. For this reason, you need to architect your technology solutions so that they enable you to rapidly support new experiences and adapt to new regions. While the right technology is key, it's critical that your strategy drives your choice of technology and not vice versa. To achieve the most effective and versatile fraud management, ultimately you need to take a holistic and business-centric view.



Contact us

Email. europe@cybersource.com www.cybersource.co.uk

CyberSource is a global, modular payment management platform built on secure Visa infrastructure with the benefits and insights of a vast \$427 billion global processing network. This solution helps businesses operate with agility and reach their digital commerce goals by enhancing customer experience, growing revenues and mitigating risk. For acquirer partners, CyberSource provides a technology platform, payments expertise and support services that help them grow and manage their merchant portfolio to fulfil their brand promise. For more information, please visit cybersource.com.

© 2018 CyberSource Corporation. All rights reserved.