
CARDNET
Fighting Fraud
in the Age of AI
LLOYDS BANK

The future of fraud prevention

Artificial intelligence (AI) is attracting growing interest and investment across a range of business sectors. Many financial institutions are putting AI at the centre of their anti-fraud strategy, a trend that is only likely to accelerate.

An increasing number of merchants are also turning to AI. This transition towards greater use of cutting-edge technology to fight fraud appears more and more necessary for retailers in the digital era.

Merchants are embracing new payment methods to give customers the greatest possible choice of how, where and when to make purchases. But this has one major drawback: more potential blind spots for fraudsters to target. By some estimates, fraud is seven times more difficult to prevent with e-commerce transactions than with face-to-face purchases.

Total fraud losses in the UK in 2017 were 5% lower than in 2016. Card fraud also fell for the first time in six years, according to UK Finance. However, e-commerce fraud against UK retailers increased 8% to an estimated £206 million. The Merchant Risk Council has warned of "an alarming new normal for e-commerce fraud". This 'new normal' is driven by online criminals themselves making ever more sophisticated use of technology, including automation, to identify vulnerabilities and maximise their gains. Figures collated by UK Finance for the first time also show £236 million was stolen last year via authorised push payment (APP) scams: those where an account holder is tricked into making a payment.

Many merchants already budget for fraud as an inevitable cost of doing business. The need to defend against potential new weaknesses is abundantly clear. Today, with the vast amount of data created relating to each transaction, AI offers hope for improving fraud detection and real-time prevention.

Key Statistics

- An estimated 90% of the world's data was created in the last two years (Source: IBM)
- Fraud losses on UK-issued cards totalled £566m in 2017, which saw the first fall in six years (Source: UK Finance)
- E-commerce accounted for 76% of total remote purchase fraud in 2017 (Source: UK Finance)
- 56% of businesses think fraud prevention solutions don't adapt fast enough (Source: Rainbird)

ANNUAL FRAUD LOSSES ON UK-ISSUED CARDS 2013 – 2017 All figures in £ millions

FRAUD TYPE	2013	2014	2015	2016	2017	% Change 16/17
Remote Purchase (Card Not Present)	301.0	331.5	398.4	432.3	*409.4*	**-5%**
Of which e-commerce	*190.1*	*219.1*	*261.5*	*310.3*	*310.2*	***0%***
Counterfeit	43.3	47.8	45.7	36.9	24.2	-35%
Lost & Stolen	58.9	59.7	74.1	96.3	92.5	-4%
Card ID Theft	36.7	30.0	38.2	40.0	29.9	-25%
Card non-receipt	10.4	10.1	11.7	12.5	10.1	-19%
TOTAL	**450.2**	**479.0**	**568.1**	**618.1**	**566.0**	**-8%**

Due to the rounding of figures, the sum of separate items may differ from the totals shown. E-commerce figures are estimated.
Source: Fraud the Facts 2018, UK Finance

Machine learning versus traditional systems

Fraud has always evolved over time as payment methods change. But the explosion of ways to pay in the present era is of a different dimension to anything seen in the past.

Retailers must beware of the potential pitfalls of omnichannel services that put customer convenience first. Now is the time to ask how new technology can help your business fight fraud, as well as close sales.

Traditionally, fraud has been tackled by applying pre-defined rules drawn up by a team of analysts. These rules require lots of manual updating as trends in fraud change. But by constantly changing tactics or mimicking good customer behaviour, fraudsters can render such responses too slow.

Machine learning (see panel) now offers a powerful alternative. It can detect suspicious patterns that may not be obvious to even the most experienced fraud experts.

As such, it may offer smarter and faster detection and prevention measures. Crucially, its capacity to simultaneously analyse huge numbers of data points provides a greater possibility of identifying new fraud techniques as they emerge – and quickly closing the gaps or even predicting the next trends.

UK Finance says £2 in every £3 of attempted fraud was stopped in 2017. But AI could raise that figure to £8 in every £10, according to Rainbird, an AI platform that uses 'cognitive reasoning'.

If this estimate holds true, the potential benefits to merchants are clearly huge. This is doubly so when you consider the current challenge of training staff to deal with fraud: 56% of merchants in Javelin Strategy & Research's Financial Impact of Fraud study said finding the time for training is a problem.

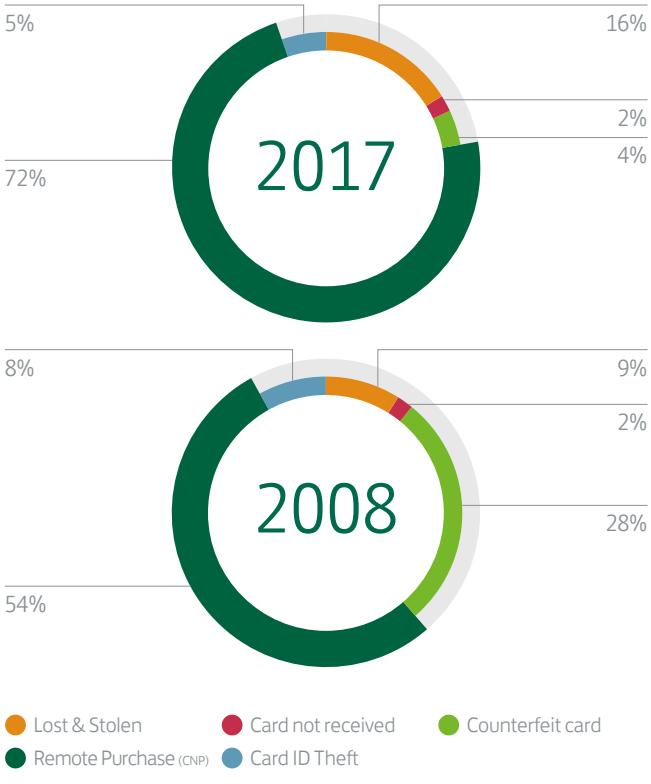
What is machine learning?

Machine learning can find hidden patterns between data points in vast streams of information without human assistance. It evolves over time through its working processes with data to become more accurate without explicit programming.

What is deep learning?

A form of machine learning based on complex artificial neural networks that mimic the architecture of the human brain.

CARD FRAUD LOSS, SPLIT BY TYPE (2017)



Source: Fraud the Facts 2018, UK Finance

Cutting false positives

Traditional fraud detection systems result in significant numbers of false alarms. The cost of investigating such cases and of delayed or lost sales is considerable. Matters may be made worse by the impact on reputation and customer trust, particularly in the social media age.

In a competitive and fast-changing environment, merchants are highly aware of such risks. According to Javelin Strategy & Research, fraud costs e-commerce merchants 7.6% of their annual revenue and false positives cost them 2.8% of revenue. By cutting false positives, AI could prove its value above and beyond the obvious advantages of reducing fraud.

PayPal's AI system offers an example of the benefits in this area. The company says traditional fraud defences would flag purchases from five different IP addresses in five days as suspicious. But PayPal's AI system might recognise the buyer as an airline pilot – thanks to its ability to process more data points – and avert a false positive.

Other companies have also reported impressive results with AI: online supermarket Ocado says it improved its fraud detection success by a factor of 15; and Danske Bank cut its false positives – previously running at up to 1,200 per day – by 60% .

Forter, a fraud prevention company, says AI can differentiate "between a customer with a complex but true story, and a fraudster who's just pretending". It does this by going beyond inflexible rules to compare a new case with every previous one it knows of. In a dynamic, data-driven world, it is impossible to fully understand risk without such technology.

Case study

Lloyds Banking Group's partnership with Pindrop

Lloyds Banking Group partnered with Pindrop, a US-based AI start-up, to detect fraudulent phone calls. Pindrop's Phoneprinting™ technology analyses 147 different features of a call to create an 'audio fingerprint'. The features include the caller's true geographic location, number history and call type.

Staff in Lloyds' customer service centres see a risk score that alerts them to likely fraud. Suspicious calls are dealt with through extra authentication requirements or passed on to a specialist fraud team.

Lloyds was the first organisation in Europe to implement the state-of-the-art technology in its call centres. Criminals use tactics such as voice distortion and social engineering to manipulate people into giving up confidential information. One in 700 calls to UK financial services contact centres is fraudulent, according to Pindrop Labs.

Hybrid solutions

Investing in AI may well be the best way for merchants to reduce the trade-off between protecting against fraud and pursuing growth. Rainbird estimates that AI decision-making on fraud could save UK businesses £7 billion over five years. But that does not make AI alone a silver bullet.

Surveys suggest retailers think automation is the main way forward on fraud. But they do not expect or want to lose the human element. Forter has warned against expecting miracles from unsupervised machine learning.

Machine learning's promise to improve over time proves it is not perfect. And fraudsters will always fight back, meaning the battle will continue to evolve. A hybrid approach therefore makes sense: one that combines the incredible and increasing power of AI with human intelligence.

RAPIDLY CHANGING FRAUD POSES TRAINING CHALLENGES
Attitudes About Fraud Management Staff (2016)

Percentage of merchants
Source: Javelin Strategy & Research

The role of people

The key question may soon be around staffing levels: how many data scientists, analysts and so forth will a company need to make the most efficient use of AI, and when would it be better to outsource? The answers will, of course, vary widely depending on the size and nature of the business.

Only a third of C-level leaders have high confidence in their organisation's ability to fight fraud, according to the Information Security Media Group. Good decision-making, as well as wider use of AI, will be needed if that figure is to improve significantly. Like so many 21st century issues, the fight against fraud now depends on humans and machines working together.

Expert Insight

Q&A with Úna Dillon, Managing Director of the Merchant Risk Council (MRC) Europe.

The MRC is the leading global business association for e-commerce fraud and payments professionals.

Q: What is the level of interest in using AI to tackle fraud among merchants and is it growing?

A: MRC Members globally see machine learning as an important move ahead in the fight against fraud. They can use AI to capture more fraud, reduce false positives, save time working fraud cases and disputes. It's a must for any e-commerce retailer.

Q: How would you describe the potential impact of Machine learning in the fight against fraud?

A: Fraud management is a balancing act as merchants constantly adjust strategies to minimise losses, maximise revenue and control operational costs. Results show businesses are succeeding in controlling direct fraud loss and merchants are manually reviewing fewer orders while rejecting approximately the same percentage of orders.

Q: How can merchants assess the effectiveness of their existing defences in comparison to the latest AI-based approaches?

A: Pre-AI usage, merchants were dependent mainly on their payment provider's fraud system. It was difficult to optimise rules to maximise sales with multiple dimensions. AI allows merchants to have control of their data and use it for their specific needs, reducing fraud and growing sales.

Q: How easy is it for merchants to integrate AI-based fraud solutions with their existing payment channels?

A: Many providers offer solutions via API that can be easily integrated. Depending on the size of the business, merchants should shop around for the best fit for them. The key is to talk to all departments before integrating an AI tool that links fraud and business teams like never before.

Q: Is there a risk that AI leaves merchants unable to understand or explain how decisions on fraud are arrived at?

A: Merchants can work with their provider to examine what problems they want to solve and build models accordingly. AI will not replace experts who continue to be required to interpret the data, provide training and influence the outcome of a model. Humans are still required!

Q: Can you give merchants any guidance on the likely cost of implementing an AI-based fraud solution?

A: Some AI tools are free. The provider may charge per click/report thereafter. Most tools are cost effective. Every dollar of fraud costs a merchant $2.94, according to LexisNexis. Using an AI tool to reduce those losses means it pays for itself in a short period of time; MRC members tell us they have seen a dramatic increase in their ability to detect and prevent fraud once a machine learning tool has been integrated into their organisation.

Important Note:

The information shared in this update was accurate at the time of publishing but many of the regulations we discussed are subject to change.

While all reasonable care has been taken to ensure that the information provided is correct, no liability is accepted by Lloyds Bank for any loss or damage caused to any person relying on any statement or omission. This is for information only and should not be relied upon as offering advice for any set of circumstances. Specific advice should always be sought in each instance.

Please contact us if you would like this information in an alternative format such as Braille, large print or audio

Our service promise
We aim to provide the highest level of customer service possible. However, if you experience a problem, we will always seek to resolve this as quickly and efficiently as possible. A copy of our 'How to voice your concerns' leaflet can be obtained by contacting the Cardnet Helpline. The complaint procedures are also published on our website lloydsbankcardnet.com/how-to-complain.

For more information visit
lloydsbankcardnet.com

LLOYDS BANK