ACI Worldwide
Real-Time Payments

The Six-Step Guide

to Leveraging Machine Learning for Fraud Management

How to utilize the smartest solutions to reduce fraud and improve customer experience

For some years now, machine learning has been a dominant emerging technology in finance.

According to 2017 IDG research, 51% of companies were using some form of artificial intelligence in their technology stack at the time. And data science solutions have been a part of major financial services innovations in trading, the use of digital assistants in banking, and underwriting for loans and insurance.

However, many industry experts believe that the pre-eminent areas in which machine learning can make a difference are payments fraud detection and prevention, and customer experience and relationships, particularly in financial services. Indeed, Gartner has discussed how more and more organizations are using machine learning to make faster decisions, while taking fraud risk into account. And McKinsey has detailed the need for banks and financiers to keep pace with fraudsters in order to protect customers and provide them with exceptional service. Or risk falling behind as their tactics become increasingly sophisticated.

Banks can use machine learning to turn the huge reserves of data they hold into customer-centric services — helping payments and fraud executives to deliver value in customer experience, as well as in customer protection. Here are six steps you can follow to introduce machine learning to your business.

> **"Machine learning is well acknowledged as one of the new technologies needed to interrogate the vast volume and variety of data within the banks' operations. Humans cannot possibly process the data at the same speed and scale. However, a bank-wide machine learning project is a huge undertaking, requiring major investment in technology and human resources."**
>
> **Cleber Martins**
> Head of Payments Intelligence & Risk Solutions
> ACI Worldwide

1 Start Simple

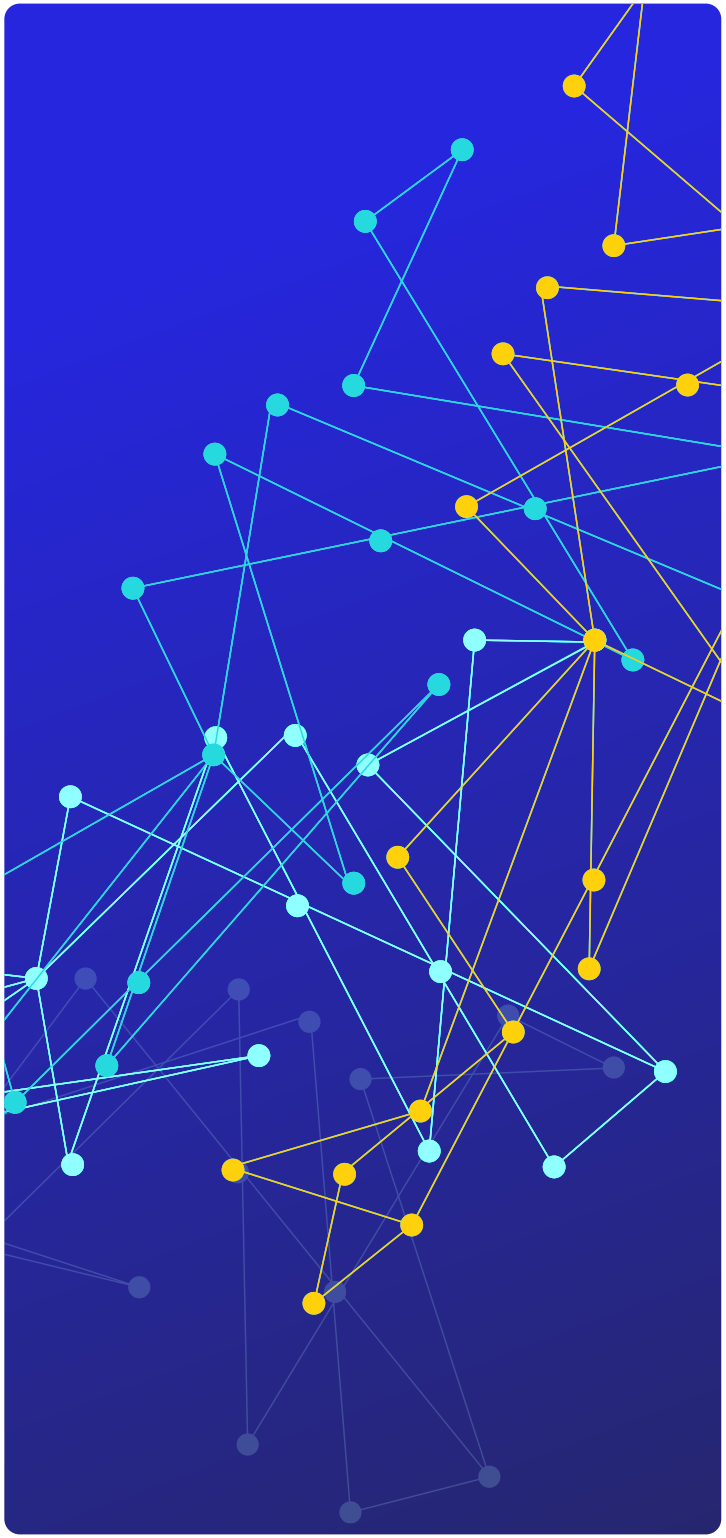
Making the right decision in real time is critical for irrevocable instant payments.

So having the right data for fraud prevention is key. This is partly why machine learning is such a crucial tool, as it understands user behavior patterns then makes decisions based on them — and the more patterns it is able to analyze, the better those decisions become.

However, if your business is introducing machine learning with no existing solutions, it can be difficult to establish large and complex models right away. Because both getting the project started and explaining decisions to senior management can be challenging.

Instead, it makes sense to begin with simple, transparent, supervised models that take into account all customer relationship data points, so you can look out for payments fraud, as well as other types of fraud. As your models become more complex, you can utilize adaptive machine learning to avoid repeated false positives, and to ensure that the model stays in line with new fraud trends.

Remember: machine learning allows for better, timely and contextualized decisions as it interacts with more data patterns. These data points can come from a complex and varied intelligence network that serves to introduce more context to every decision. So over time you'll see how it can enable better customer experience, smarter product recommendation and more frictionless banking services for users.



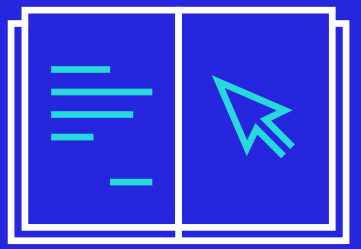
2 Prioritize Real-Time Payments

Real-time payments (RTP) availability is expanding around the world — driven by customer demand for convenience, choice and speed of access to funds.

Governments, regulators and banks are all encouraging adoption among consumers and merchants, with particular strides made in India, the U.K., Japan and Australia. In real-time payments, the window for fraud prevention is much shorter and the ability to recover a fraudulent payment is much lower.

Finance institutions looking to utilize machine learning and artificial intelligence solutions should consider how they apply it for RTP. Doing so requires sophisticated data management; your platform will need to absorb data, perform machine learning and provide actionable results. You also need to build strategies to be successful, and have the right controls in place, such as the flexibility to build strategies and rules around an enterprise view of a customer in real time. And, you'll need to action according to calculated risk — quickly approving genuine activity, declining high-risk payments and deferring "middle ground" situations where additional data is required to authenticate and authorize the payment.

Not only is protecting RTP important from a customer experience perspective, it's important from a fraud one, too. Fraudsters always target new payment types, but banks can overcome this with the right strategies and solutions. The fraud rate for traditional push payments made in U.K. Faster Payments (UKFP) is now lower than credit cards (0.007% for UKFP in 2013, compared to 0.063% for cards).*



Keeping Pace with Innovation in Real-Time Payments

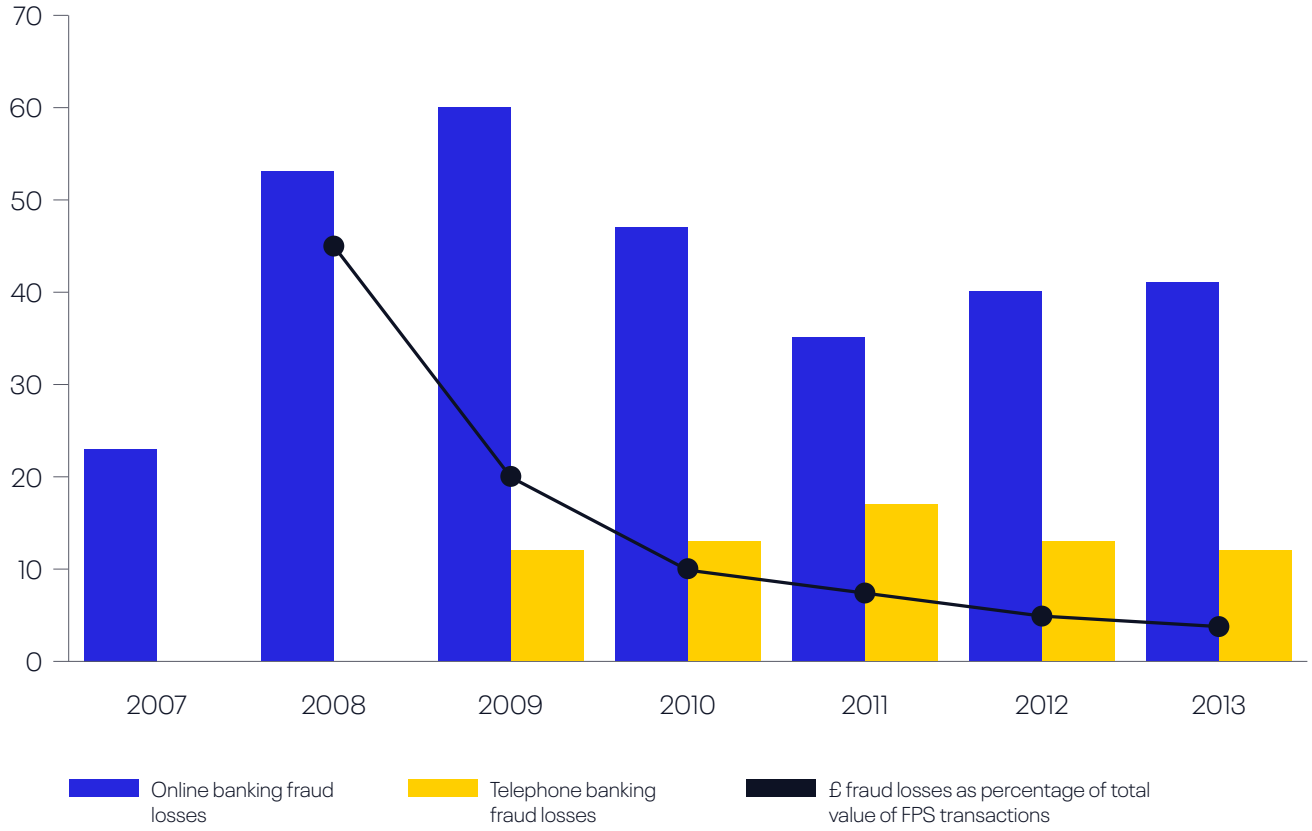
Find out more about becoming real-time ready in our **Keeping Pace with Innovation in Real-Time Payments** eGuide.

Find Out More

*Source: Payments Council and FFA UK

U.K. Faster Payments Fraud Losses

Fraud has declined from £1.6 per £1,000 in 2008 to just 7p per £1,000 in 2013.



*Source: Payments Council and FFA UK

Learn more about how to prepare fraud prevention for new payments in our expert analyst webinar.

ACI® Fraud Management™ solution gathers rich data via APIs for improved decisions in real time via adaptive machine learning, visual exploration of the data and analytics. It supports you in developing decisioning strategies in order to support the business.

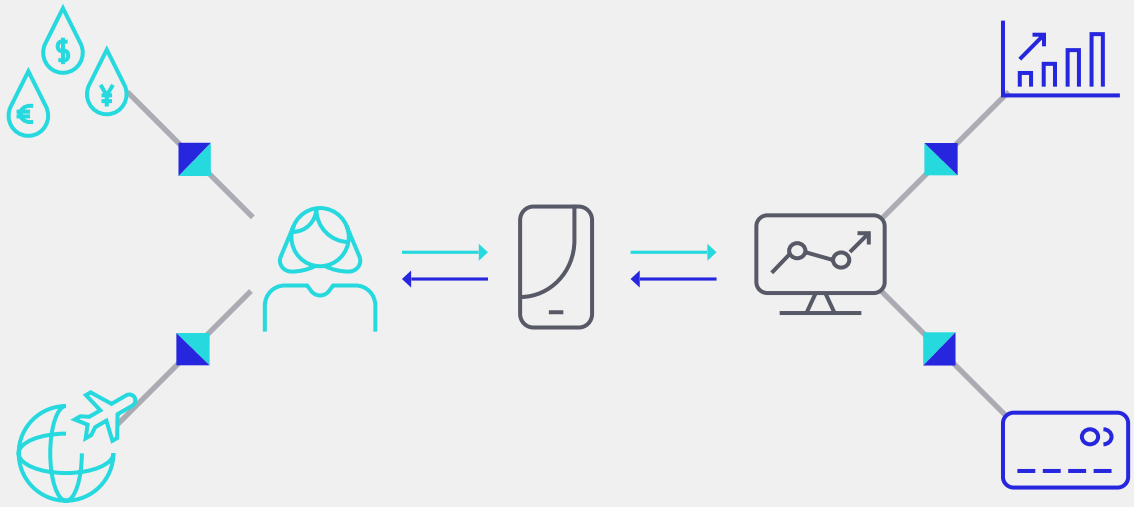
3 Use Data from the Payments Stream

Banks are fortunate in that they have more data on their customers than ever before.

They must look to provide both exceptional customer experience, and solid fraud defenses based upon this, moving towards greater fraud management.

To do this, banks should look to use the full breadth of data that already exists within their payment streams, leveraging fraud prevention data inputs. Then match that against the customer profile, such as known device, travel information and credit limits.

This will minimize the false positives that can harm the customer experience, so you'll be guarding against fraud, at the same time as enhancing the experience you deliver.



Banks know when customers are traveling, and when the customer is reaching their credit card limit. They can use this insight and existing two-way communications to seamlessly offer and confirm acceptance of an overdraft extension or credit card limit increase. The customer avoids unnecessary fees and feels well served by the bank.

4 Add Fraud Markers for Adaptive Machine Learning

For machine learning to work to its utmost potential, models need constant interaction with their environment — reinforcing lessons learned so the solution becomes better at detecting fraud over time.

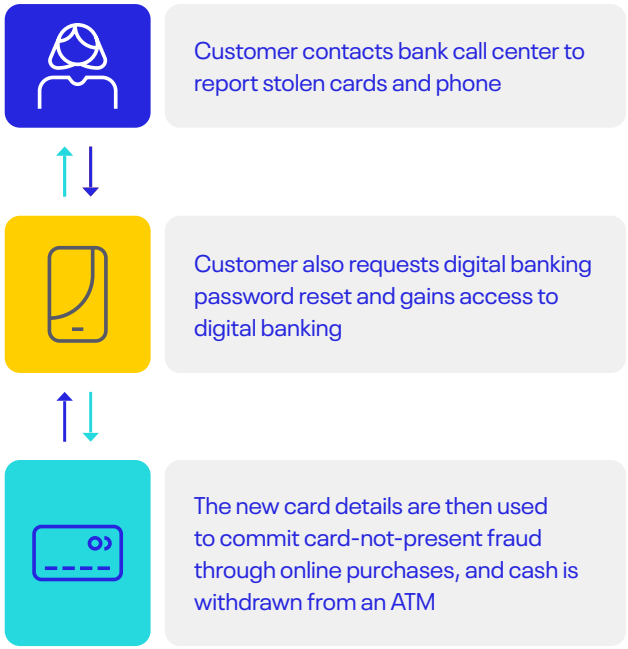
This is why it's so vital for banks to add fraud markers as they come about. Today, tools can be set up to learn from additional markings fraud analysts see on customer accounts and "adapt" by changing the weight of evidence (WOE) within the affected features. These markings could be erratic spending patterns by transaction value or velocity, or by merchant type — anything that indicates a fraudster may be "testing" payment instruments.

Models can improve and learn from these new fraud patterns, supervised by a human who is adding the new data.

5 Bring Card, Non-Card and Digital Together

Payments fraud takes place in a number of channels.

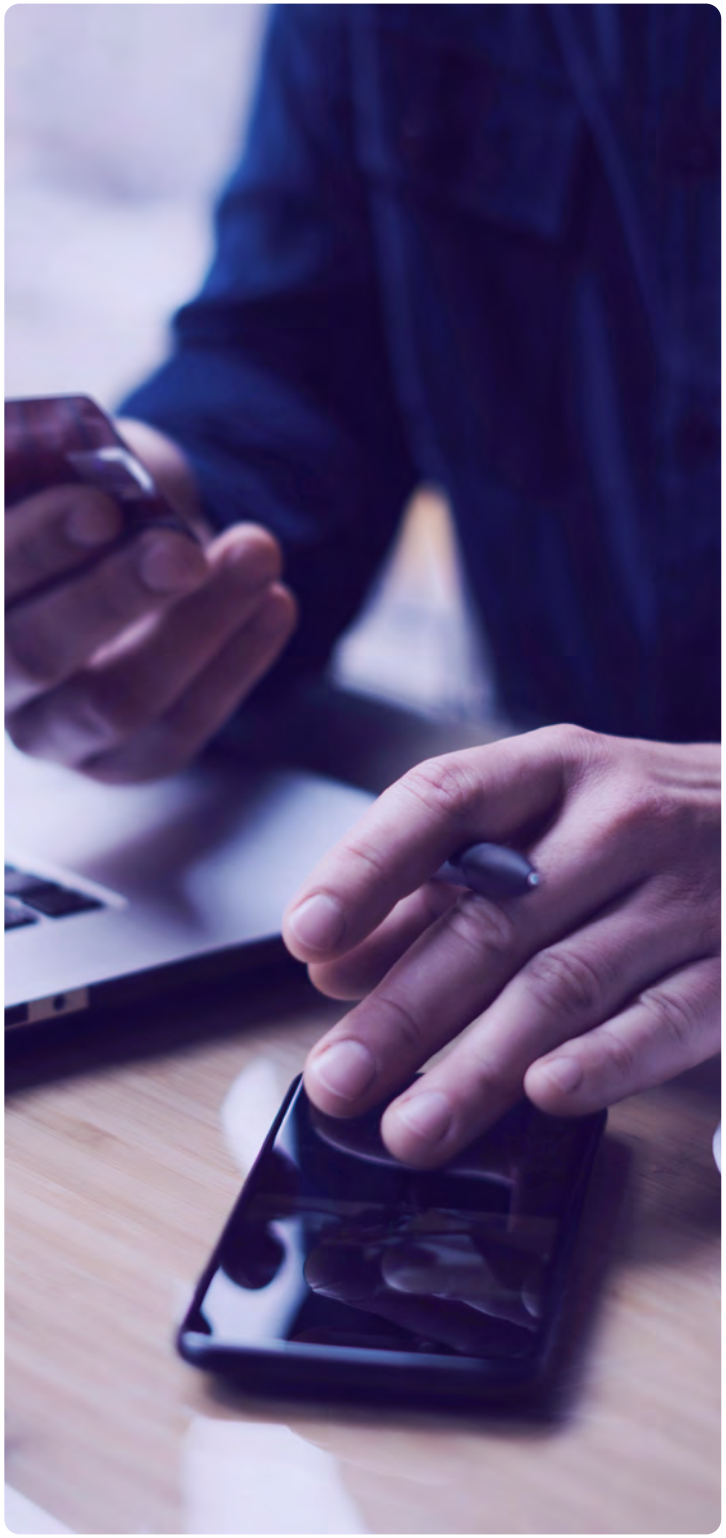
And the risk that's present in each magnifies as fraudsters' methods become more sophisticated, and consumers use new, innovative payment services. As does the risk of cross-channel fraud, as the graphic shows.



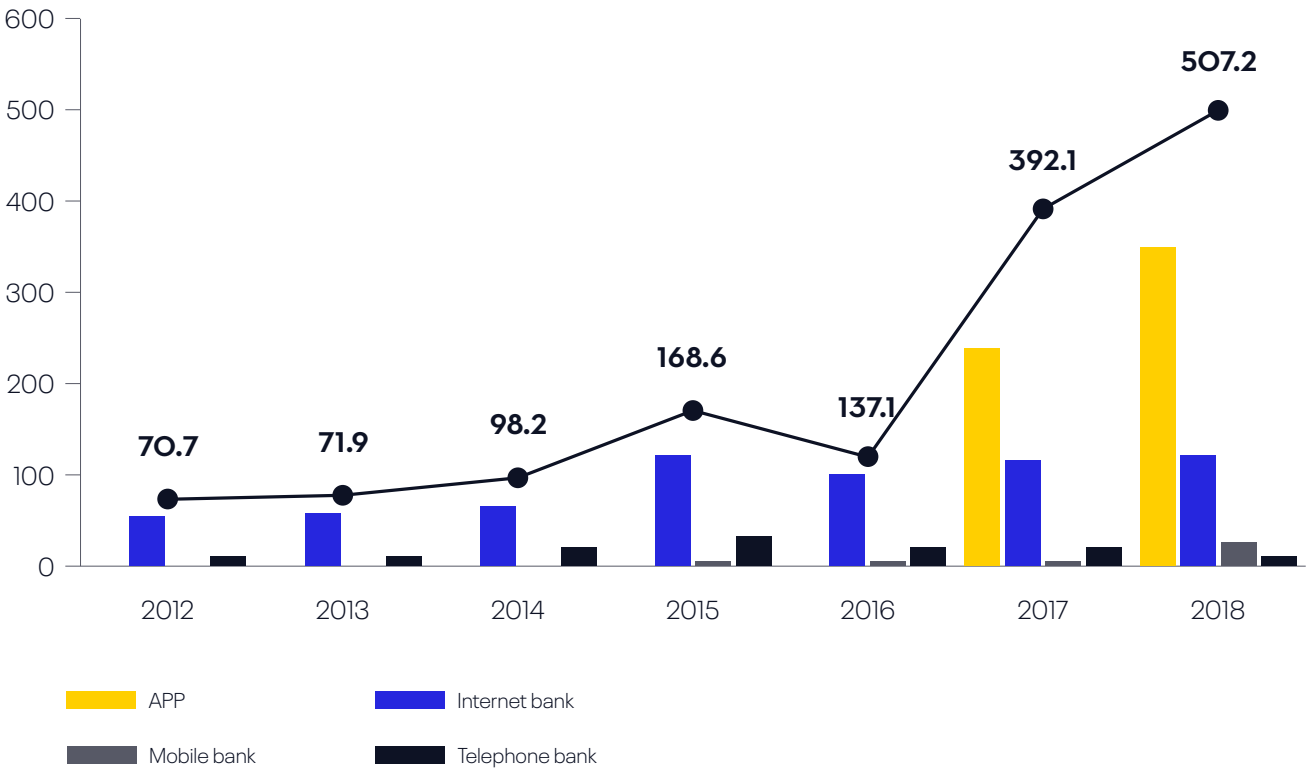
To give machine learning its best chance of aiding fraud defenses, it's sensible to bring the data that these channels provide together.

Firstly, this delivers an enterprise view that helps banks build up an accurate, insight-led picture of their customer — meaning better service, and fewer false positives in fraud detection. Secondly, it helps them to understand the fraud vectors that might affect the bank's business — and the more customer data they have to work with, the better they can understand the detail of those vectors.

It's also important to prioritize fraud prevention as new channels come into use, otherwise investment in emerging payment types could be put at risk. As the graph on the next page shows, innovation often precedes security — which creates huge problems for banks.



U.K. Remote Banking (Non-Plastic) Fraud Gross Losses (£MN)



Source: UK Finance

Non-plastic fraud (primarily Authorized Push Payments) is significantly increasing in the U.K., as fraudsters use more sophisticated techniques to target customers outside of the transaction itself.

6 Input Data from Intelligence Network

The cause and effect of financial fraud are both wide-ranging. Almost nothing happens in isolation. Now, financial institutions are better able to protect both their customers, and their customer experience, through a network of verified solutions and partners that complement and bring time to value for risk management.

This involves data management and orchestration through bringing sources and risk services together for protection across the financial ecosystem. As well as using machine learning for advanced analytics, decisioning and business intelligence.

It's common sense to think of fraud protection as a task to be tackled from multiple angles — now doing that is achievable for all financial institutions.

"Beyond stopping new account fraud, creating a behavioral biometrics profile of the account holder is an effective way of preventing account takeover attacks. BioCatch uses behavioral data specific to the customer to identify whether the enity entering the data into the digital channel is the actual owner."

From Data to Decisions

Over the past few years, banking and payments have become a data-dependent and data-driven industry.

Now, innovation in payment products and services is accelerating this trend. The upside of this is that there are now more ways to reach, engage and interact with existing and potential customers than ever before. The downside is that the risk of fraud is immediate, growing and evolving. As well as being less recoverable for many institutions.

To improve customer relationships, and to minimize fraud, banks are bringing machine learning technologies into their businesses, using the data available to them to protect their customers and better serve them. It's all part of the journey that will bring about fraud reduction, frictionless experiences and greater payments intelligence for added value in customer relationships. And it's why machine learning will become essential to delivering fraud-prevention in the coming years — for those that haven't yet invested in it, the time is now.

Westpac

Find out more about how ACI can work with you to reduce fraud and improve customer experience with machine learning in our Westpac New Zealand case study

Read Case Study

ACI Worldwide
Real-Time Payments

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ABR1196 04-21