Using AI and collaboration to prevent consumer payment scams

WHITEPAPER

Innovation is key to progression in every area of life, and in our ever-changing digital world it's the vital ingredient needed to ensure our security capabilities remain two steps ahead of those who wish to disrupt our digital economy and damage the trust it is built upon.

"By leveraging data points and technology from different areas of the business, Mastercard is uniquely suited to meet this moment and help make the payments ecosystem safer and more secure."

– Jonathan Anastasia, executive vice president, Crypto and Security Innovation

Overview

Just as payments have progressed from cash to cards to mobile devices and beyond, financial security must continue to grow to protect this increasingly complex ecosystem.

As the ways we send money grow and evolve, so do the ways fraudsters attempt to steal it. The advent of digital technology, while a net positive, means that fraudsters and scammers are able to utilize broad-reaching digital communication channels (e.g., mobile banking, text, phone) to manipulate consumers into providing their account credentials and making fraudulently induced payments.

They're harnessing the scale of the digital economy and the intimacy of social media to find and prey on unsuspecting people – whether it's fictitious online deals, urgent alerts sent by seemingly legitimate institutions, or false promises of romance, impersonation scams of all kinds have plagued people and businesses over recent years and shaken the confidence of those affected.

Prevention is, of course, the ideal strategy to combat these scams – and Mastercard is using AI-powered insights, trained on billions of transactions and data points, to help financial institutions protect their customers and halt the flow of stolen money by identifying scams before the funds are sent.

By leveraging data points and technology from different areas of the business, Mastercard is uniquely suited to meet this moment and help make the payments ecosystem safer and more secure.

Jonathan Anastasia
Executive vice president, Crypto and Security Innovation

A rising threat

$5.25b

estimated cost of scams in the U.S., U.K. and India by 2026

85%

of financial institutions in the U.S. expect fraud attacks to increase due to the rise of real-time payments

"Spotting fraudulent payments among millions made every day is like finding a needle in a haystack, with scams becoming ever more complex."

– Paul Davis, director of fraud prevention, TSB Bank

Scams are a form of financial crime in which an individual is manipulated or deceived into either making a payment to a fraudster or handing over their credentials, so that the fraudster can bypass typical security measures. Scams are currently one of the largest and growing risks facing financial institutions globally, and are predicted to cost $5.25 billion in annual losses across the U.S., U.K. and India by 2026.

Scammers adopt many different social engineering techniques to perpetrate their illicit activities, posing as everything from bank employees to potential romantic partners in order to gain a person's trust and, ultimately, their financial information. Cyber attacks, such as phishing and smishing, are also commonly used to gain personal information that can then be used to commit fraud.

Take Mandy (pseudonym), for example. A social worker by trade, she was using a dating app when she came across Avery – a boxing promoter and divorced father of one. Avery told her all about his job, the excitement of putting matches together and his efforts to invest in female boxers. He seemed passionate about his work and completely smitten with Mandy as well.

But Avery ran into trouble when some new furnishings he was waiting for to renovate his boxing club got held up at U.K. customs. With all of his free cash invested in deals, he didn't have the money he needed to clear the goods. So he turned to Mandy to see if she could lend him the £6,000, and she reluctantly agreed.

Avery seemed to run into a lot of similar troubles over the course of their relationship – by the time it ended six months later, Mandy had lent him a total of £60,000. Of course, Avery had no intention of paying this back, because he was never a real boyfriend – he was a romance fraudster.

Mandy is far from alone in being targeted for this kind of scam: 85% of financial institutions in the U.S. are expecting fraud attacks to increase in response to the rise and ease of real-time payments.

But awareness alone is not enough to for banks to track down and stop these kinds of criminals. Spotting fraudulent payments among millions of transactions is like "finding a needle in a haystack," as Paul Davis, director of fraud prevention at U.K.-based TSB Bank, puts it.

Because people who fall prey to scammers send the money themselves, the fraudster doesn't need to break any security measures in order to get the funds – which makes these acts incredibly difficult to identify and prevent. By the time people realize they've been scammed, they have already sent their money.

Leveraging a global network

Once fraudsters and scammers obtain someone's funds, they move them at speed through a series of so-called "mule" accounts to disguise them. For the past five years, Mastercard has worked with U.K. banks to follow the flow of funds through these accounts and then close them down.

This meticulous tracing has yielded millions of fraud and money laundering data points each year from countries around the world. Now, data points like account names, payment values, payer and payee history, and the payee's links to accounts associated with scams allow Mastercard's new anti-scam solution to provide banks with profiling built and pre-trained on billions of transactions.

The solution, called Consumer Fraud Risk, uses AI-powered insights to help banks predict scams in real time and before any money leaves a person's account. It is trained on years of transaction data and helps predict whether someone is trying to transfer funds to an account affiliated with these kinds of authorized push payment (APP) scams.

Consumer Fraud Risk is powered by Mastercard AI.

A continuous fraud feedback loop trained by machine learning ensures the solution constantly evolves, adapting to new developments in the fraud landscape. In milliseconds, a risk score with insights is returned to the financial institution before a payment is sent, which the financial institution can then use to make a real-time decision on whether to proceed with the payment.

1. Growth in APP Scams Expected to Double by 2026." ACI Worldwide and GlobalData, 2022.

£100m

estimated annual savings by rolling out Consumer Fraud Risk U.K.-wide

Driving results with AI

Since implementing Consumer Fraud Risk in July 2023, U.K.-based TSB bank has seen a 20% increase in detection of APP fraud, which Davis calls one of the biggest improvements of any individual fraud prevention project he's worked on.

TSB estimates that if the solution was rolled out across all banks in the UK, it could save U.K. banks about £100 million per year.

Because of Mastercard's experience in tracing and stopping financial crime across the U.K.'s real-time banking system, the country has been a natural first place to roll out Consumer Fraud Risk. The solution is now live with eight other U.K. banks in addition to TSB, including Lloyds Bank, Halifax, Bank of Scotland, NatWest and Monzo – and soon rolling out to other markets around the world.

Mastercard is in discussions with potential clients in markets with mature real-time payments systems and significant APP fraud. Initial results from banks using Consumer Fraud Risk's score show great success in preventing scams. It has helped banks to create targeted fraud strategies that clearly identify different types of scams, especially when used in conjunction with other insights regarding customers and their behavior.

"It's a good example of the power of sharing data," Davis said. "It's the first time we've been able to see both sides of the payment – sending and receiving."

Increasing visibility gives banks the information they need to make the right calls. To learn more about Consumer Fraud Risk, how it works, and the impact it's having on financial institutions, reach out to your Mastercard representative or visit https://b2b.mastercard.com/financial-crime-solutions/.

2. Figure is calculated from UK Finance Annual Fraud Report data for 2022 in which £485.2 million was lost to APP fraud. Based on TSB's percent increase in detection and scam payments prevented, £97 million would be saved across the banking sector based on latest UKF data.

For more information visit
b2b.mastercard.com/financial-crime-solutions/