Prevent business payment fraud

FINANCIAL CRIME SOLUTIONS

OCTOBER 2019

Contents

3 The issue of business payment fraud

4 Introducing our solution to prevent business payment fraud

7 Real insights to enable right decisions

8 Delivering measurable benefits

9 Live service: Preventing business payment fraud with NatWest

11 Financial crime solutions

The issue of business payment fraud

Fraudsters actively target various types of payments to fund criminal activities, in the process stealing money from people, businesses and government departments. This causes significant financial distress at an individual, company and economic level, as well as costing billions each year.

A significant threat to business customers is payment-related invoice fraud. This includes CEO fraud (also known as business email compromise or BEC) and invoice redirection, all of which are high-value frauds where companies are duped into paying money to a fraudster rather than a legitimate supplier.

Once processed, the funds are quickly laundered through the banking system, making it difficult to trace. Stolen funds are rarely recovered, leaving financial institutions and their customers to bear the cost. Often, this directly impacts the company as it still owes the invoiced amount; some businesses do not survive the loss and people lose their jobs.

If these misdirected payments are detected early in the cycle, they can be stopped before reaching a fraudster's destination account – saving financial institutions and their customers considerable amounts each year, and reducing the level of distress experienced as a result.

Mastercard's solution to prevent business payment fraud identifies and flags transactions matching this behaviour by applying advanced analytics and behavioural rules to payments data.

Introducing our solution to prevent business payment fraud

We enable financial institutions to prevent business payment fraud by using advanced, machine-learning and behavioural analytics to determine whether a payment is high risk before it is completed.

Our algorithms analyse potentially tens of millions of transactions a day to identify high risk payments which fit the characteristics of these types of frauds and deliver a manageable number of alerts and/or risk score responses, precisely tuned to a customer's preference. The alerts are rank-ordered by potential risk so clients can prioritise investigation activities. The accuracy of the solution (built on historical payment data) minimises the incidence of false positives. We alert on a tiny fraction of one percent of all transactions while still managing to detect high levels of fraud.

The solution consists of advanced analytical models, which are trained using the most current machine learning techniques. As new patterns of fraud emerge, the models adapt to changing behaviour via supervised learning, using new fraud and legitimate data to recognise slight alterations in attacks. Additionally, behavioural classifications can be tuned to exclude low risk payments to avoid flagging transactions which do not fit the behaviour of a fraudster.

Our solution identifies:

Invoice redirection fraud

This fraud occurs when the beneficiary account number is different from prior history between beneficiary and payer due to a fraudster duping a business into redirecting the regular payment details to the fraudulent account;

New relationship fraud

This fraud occurs when there is no payment history between payer and beneficiary, i.e., the beneficiary account has not been seen before and there is no payment history with the beneficiary name. Fraudsters often do this by either intercepting the first invoice to a new supplier or by convincing finance teams to pay a bogus invoice. A key attack that can be identified with these alerts is CEO fraud, which is currently an extremely high profile and damaging type of fraud.

Fraudsters are exploiting the benefits of payments systems to steal money with devastating efficiency. Businesses that fall victim to new relationship and invoice redirection fraud lose money and sometimes, are forced to close as a direct result. Financial Institutions are affected by the damage this has on their relationships with business banking customers, at times absorbing all or part of the loss, and the negative impact it brings to operational efficiencies.

These types of fraud are low risk and high reward for criminals and are rising year-on-year.

At Mastercard, we apply cutting-edge data analytics to the information generated through bank account-to-bank account payments. In the UK, for example, the amount of data created amounts to more than 11 billion yearly transactions with a total annual payments value of £6 trillion.

Our solution to prevent business payment fraud is powered by this fact-based, timely and large-scale payments data-set comprising over 18 million business payment fraud data points. It provides additional insights which complement financial institutions' existing solutions and capabilities. Our data analytics-led solution has the capability to identify and flag likely incidences of payment related fraud before the funds leave a victim's account, giving the financial institution time to intervene, contact their customer, and stop the transaction before the funds are lost forever.

70%

of businesses believe payment fraudsters are 'ahead of the industry'

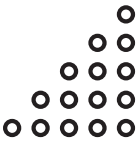
Mastercard global business fraud report 2018–2019

Leverage the power of high volume, high quality payment data

- First time total view of end-to-end payments data
- Tens of millions of payments added into the system every day
- Billions of historical transactions can be used for profiling

Analysis and generation of precision insights

- Cutting-edge, machine-learning technology
- Specialist data science team
- 2-layer analytical approach — behavioural-based plus machine learning



Robust fraud detection results

- Pinpoints the potential fraud amongst tens of millions of transactions
- Flagged by value and risk
- Rapid detection and quick to action

26.2 US billion

Global loss to business email compromise (BEC) fraud between October 2013 and July 2019.

Source: FBI Public Service Announcement, 2019

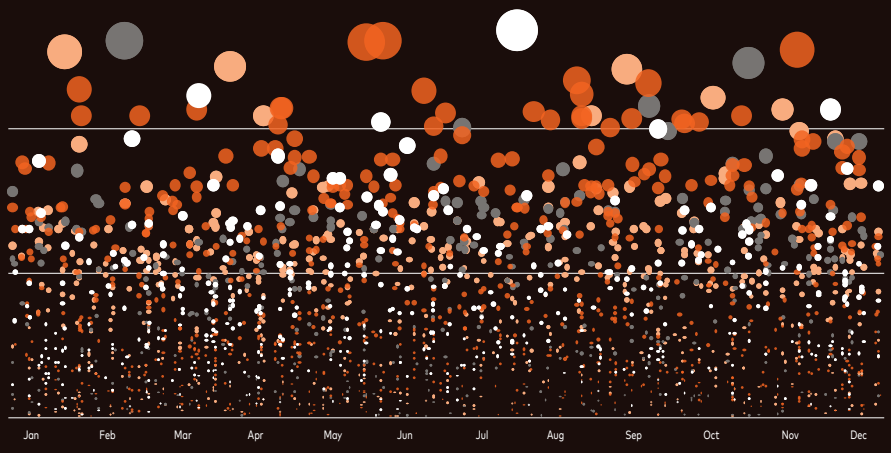
Real insights to enable right decisions

Our ability to prevent business payment fraud is based on the analysis of payments data. The output takes the form of scores and alerts which are sent securely to individual financial institutions, identifying potentially anomalous transactions.

The alerts are generated regularly, based on customer preference and payment system schedules, and summarise information with risk flags, scores and payments data.

They include information such as:

- Flags to identify key risks that are present in a transaction/ relationship;
- A score to help analysts prioritise work;
- Payment details to ensure an analyst can work and adjudicate an alert efficiently with minimal need to use internal systems.



10 billion

lost to business payment fraud every year

Source: Tungsten Network research

Delivering measurable benefits

Our solution to prevent business payment fraud uses advanced, machine-learning and behavioural analytics to determine whether a payment is high risk. For financial institutions, the benefits are clear.

1

Low systems integration

Our business fraud solution is a centralised service, meaning that the solution can be accessed with little IT integration effort. Secure scoring and alerts can be up and running within weeks.

2

Cost protection

The robust analytics and machine learning underpinning the solution enables financial institutions to more quickly and effectively identify potential fraudulent transactions and take immediate action to avoid losses. This also delivers potentially significant operational efficiencies for financial institutions, in particular a reduced impact on resources and time from a customer service perspective by intercepting suspect fraudulent payments before they occur.

3

Safeguard reputation

Our solution to prevent business payment fraud enables financial institutions to act more quickly to protect their business banking customers from losing money to fraudsters. Feedback from our customers is that it helps build a higher level of confidence and trust in the financial institution, and creates positive customer engagement by contacting businesses before a high-risk transaction leaves their account.

CASE STUDY

Live service: Preventing business payment fraud with NatWest

A powerful new solution to fight financial crime

Together with NatWest, Vocalink, a Mastercard company piloted a new approach to preventing business payment fraud using cutting-edge machine learning and analytics.

Starting in Q1 2017, Vocalink's data scientists and product team worked closely with NatWest analysts to define fraud attack scenarios. They used this to build a machine learning algorithm, trained and fine-tuned the model, and then tested it against one year's worth of data in which known frauds were hidden. The final in-flight detection rate was over 90% and included some incidences that were previously unknown.

Our solution to prevent business payment fraud went live with NatWest in October 2017. As of September 2019, it had prevented losses of £14.5 million to customers such as charities and schools, with notable examples including a CEO & BEC fraud of almost £40,000 and an invoice redirection fraud of over £200,000.

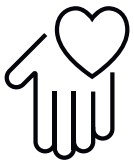
It was awarded National Technology Awards 2018 'Analytics Project of the Year', Retail Banker International 2018 'Banking Security Innovation of the Year', and Card & Payments Awards 2019 'Best Security or Anti-Fraud Development'.

"Following its introduction, the solution has prevented losses of over £12.5 million to customers, with individual attacks often worth hundreds of thousands of pounds.

It is part of our on-going commitment to fighting payments-related fraud on behalf of our customers, helping businesses to stay safe and secure."

— Lee Fitzgerald, Head of Fraud for Commercial and Private Banking at NatWest, April 2018

Notable successes



A charity

- Tricked into paying a false invoice to a builder
- The invoice was fw00
- The customer had never paid this builder in the past
- We flagged the payment and the bank was able to follow up quickly
- The charity was able to cancel the payment

A construction company

- Submitted an invoice of over £200,000 for payment to what they thought was an existing supplier
- We identified and flagged the fraudulent payment
- Because fraudster was so convincing, when the customer was contacted, the bank had to work hard to convince them that it was highly likely to be a fraud
- When they finally investigated and validated the fraud, they couldn't believe they had been caught out – and were delighted that their bank had protected them from losing their money

Financial crime solutions

Our award-winning financial crime solutions help our customers better verify payment requests and recipients and prevent financial crime before it occurs. Our network-level solutions allow us to trace illicit funds across the payments network and alert financial institutions to suspect mule accounts so they can investigate and close them down. They can be engaged either at individual bank or scheme level, or across entire payment networks anywhere in the world.

For more information

vocalink.com/financialcrimesolutions
info@vocalink.com

Contact us
info@vocalink.com
vocalink.com

Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom

740053/01.050919

DESIGNED BY NPP CREATIVE