OPEN BANKING EXPO

RISING TO THE FRAUD CHALLENGE 2024

IN ASSOCIATION WITH

Bottomline

ABOUT

OPEN BANKING EXPO

Open Banking Expo is a global community of Open Banking and Open Finance executives responsible for digital transformation across the financial services sector. The brand organises face-to-face and virtual events in the UK, North America and Europe, which includes its flagship Expo and live panel debates, throughout the year.

Open Banking Expo also hosts a leading industry podcast 'Open Banking Expo Unplugged' and online news resource dedicated to Open Banking and Open Finance, as well as the latest developments in payments and data.

The company curates the Global Open Banking Partner Directory, showcasing industry expertise from around the world. In addition, it regularly collaborates with international thought leaders on surveys and reports to harness and evaluate the latest sector developments, and to offer industry analysis and overview of the biggest hot topics across the globe.

For more information visit **www.openbankingexpo.com**
𝕏 @OpenBankingExpo
in Open Banking Expo

Bottomline

Bottomline helps businesses transform the way they pay and get paid. With over 30 years of experience moving more than $10 trillion in payments annually, Bottomline is dedicated to reimagining business payments and delivering solutions that add value to business and financial institution customers globally.

More specifically, Bottomline's SaaS-enabled payments, securities, connectivity, and financial messaging solutions are trusted by over 600 clients globally, leveraging multiple domestic and cross-border payment networks and schemes with a track record of success.

For more information visit **www.bottomline.com**
in Bottomline

CONTENTS

INTRODUCTION

Ellie Duncan
head of content
Open Banking Expo

AMID AN EVOLVING FRAUD LANDSCAPE, OUR REPORT ENDEAVOURS TO OFFER CRITICAL INSIGHTS INTO EVERYTHING YOU NEED TO KNOW ABOUT FRAUD MONITORING AND PREVENTION

> "As the scale and scope of fraudulent activity has increased, so too has the sense of urgency to tackle it"

Open Banking Expo and Bottomline are pleased to bring you this report, 'Rising to the Fraud Challenge', which takes a deeper dive into the global fraud landscape through insights from senior executives at Bottomline, the latest industry statistics and a contribution from Pay.UK.

Across financial services, fraud has always been a risk management priority for organisations and businesses. However, as the scale and scope of fraudulent activity has increased, so too has the sense of urgency and the wherewithal to tackle it.

Fraud detection and prevention is top of mind for the industry across payments, Open Banking and lending.

And there are signs that the financial services industry's efforts are paying off. UK Finance found that, in 2022, there was an 8% reduction in the amount stolen through fraud, totalling £1.2 billion. Across the UK, the number of fraud cases was down 4% to nearly three million cases.

The decline continued into the first half of 2023, when UK Finance reported that £580 million had been stolen by criminals – a 2% decrease compared with the same period a year earlier.

But, now is not a time for complacency. While advancements in UK and EU regulation, Open Banking, AI and machine learning are helping to identify and interrupt attempts at fraud, these same technological developments are enabling scammers to blur the lines and trick consumers into sending money to them.

Bottomline's Omri Kletter writes about the imperatives for payments professionals against this evolving fraud backdrop, see Page 6. He reveals what tools have emerged as critical components to maintain payments speed and security.

Integrated suites of fraud solutions and the indispensable role they play in safeguarding are the focus of Ruud Grotens' article, on Page 11.

Authorised push payment (APP) fraud is a growing threat in the UK, but one that is being addressed by the emergence of Confirmation of Payee, as Bottomline's Mark Bish and Erez Nounou consider, on Pages 14-15. This theme is picked up by Pay. UK's Kate Frankish later in the report, as she writes about how CoP is being deployed in the fight against fraud, on Page 18.

What are the lessons learned from CoP and how has discourse shifted to a broader narrative of fraud prevention? Read more on Page 16. Read more about the UK's experience and leadership in fraud prevention, as well as the role of SEPA Instant and ISO 20022 in fraud mitigation, on Page 17.

We hope you find the report as informative and insightful as it was to research and write.

TOTAL AUTHORISED PUSH PAYMENT FRAUD

Source: UK Finance, 2023 Half Year Fraud Update

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	% Change 2022–23
Cases	69,093	85,521	101,540	94,456	95,167	112,205	116,324	22% ↑
Payments	105,069	139,502	172,622	172,515	166,327	205,939	211,558	27% ↑
Gross loss	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	-1% ↓
Returned to victim	£75.0m	£99.7m	£125.8m	£131.9m	£135.6m	£150.0m	£152.8m	13% ↑

NAVIGATING THE GLOBAL FRAUD LANDSCAPE: IMPERATIVES FOR PAYMENT PROFESSIONALS

Omri Kletter
global vice president, product and strategy – risk solutions
Bottomline

BOTTOMLINE'S OMRI KLETTER EXPLAINS HOW ORGANISATIONS CAN ADAPT TO MEET THE RISKS AND THREATS IN AN EVOLVING FRAUD LANDSCAPE

In the dynamic realm of global payments, where efficiency, security, and customer satisfaction are paramount, the battle against fraud is a pivotal challenge.

UK Finance reported fraud losses reaching £580 million in the first half of 2023. It is crucial for payment professionals to have a deep understanding of the evolving fraud landscape, including the growing threat of authorised push payments fraud.

To achieve the objective of improved operational efficiency, cost reductions, and surpassing customer expectations it is vital to have fraud prevention front and centre. The synergy among these objectives underscores the interconnectedness of effective fraud mitigation strategies. By implementing robust fraud solutions, businesses streamline operations and mitigate the risk of false positives, bolstering efficiency and reducing operational costs.

Let us not forget that the imperative to exceed customer expectations directly corresponds to any organisation's fraud prevention efforts. Reducing fraudulent activities translates to heightened customer satisfaction, fostering trust and loyalty, while attracting new clientele and minimising attrition rates.

Laying the foundations

In the era of real-time payments, speed is of the essence. But accelerating payment processes must align with efforts to combat fraud. Pre-verification and sanction screening emerge as critical components, ensuring the integrity of instant payment mandates.

"Scalability and innovation form the bedrock of future-proofed fraud prevention strategies"

Transparency and cash visibility are indispensable facets of fraud prevention. Leveraging data-rich standards, like ISO 20022, empowers fraud departments to discern anomalies and detect potential fraud patterns with greater precision.

Scalability and innovation form the bedrock of future-proofed fraud prevention strategies. By harnessing advanced technologies for analytics and risk management, organisations can swiftly identify emerging fraud patterns and adapt to evolving threats. Nevertheless, the human element remains indispensable, augmenting technological solutions with nuanced expertise.

Adherence to regulatory mandates and global compliance standards is non-negotiable. The imperative to combat nefarious actors necessitates the sharing of best practices and the adoption of industry-wide mandates such as Confirmation of Payee and Verification of Payee.

Achieving interoperability on a global scale underscores the importance of standardised fraud prevention practices. Arguably, strong customer authentication within Open Banking should reduce fraud. However, lacklustre adoption driven by the lack of standardised APIs has curtailed progress. Effective communication across the payment ecosystem hinges upon universal adherence to best practices and global standards.

In partnership with Bottomline, organisations from corporates to financial institutions benefit from comprehensive fraud expertise across the payment ecosystem – from sanction screening to secure payments and Confirmation of Payee – which allows them to proactively mitigate risks, uphold regulatory compliance, and safeguard financial integrity.

As the global landscape continues to evolve, payment professionals must remain vigilant, adapting their strategies to confront emerging threats and uphold the integrity of the payment ecosystem. By embracing a multifaceted approach to fraud prevention, organisations can navigate the complex terrain of global payments with resilience and confidence.

INDUSTRY DEVELOPMENTS IN THE FRAUD SPACE

Ellie Duncan
head of content
Open Banking Expo

BIG TECH, OPEN BANKING, AI, COP AND THE REIMBURSEMENT REQUIREMENT – WHAT DOES IT ALL MEAN FOR THE FUTURE OF FRAUD?

Fraud is a growing threat to businesses and, by extension, their customers. It is a highly complex and sensitive issue, but one that is being increasingly addressed by services such as Confirmation of Payee in the UK, and by transparent reporting of fraud volumes and cases.

According to the National Crime Agency, the most common types of fraud are payment diversion fraud, investment fraud, romance fraud, courier fraud, as well as cheque, plastic card and online bank account fraud.

Andy Donald, director of communications at UK Finance, confirms that fraud continues to be one of the most prevalent crimes in the UK.

"Typically, criminals first focus their attempts on socially engineering personal information from their victims with a view to committing authorised push payment (APP) fraud in which the victim makes the payment themselves," he explains.

"If this is not successful, the criminal often has enough personal information to enable them instead to impersonate their victims, with a view to either taking control of their existing accounts or applying for credit cards in their name."

In its Half Year Fraud Update 2023, UK Finance reported that APP fraud fell in the first half of 2023, down 1% to £239.3 million. However, it was still 27% higher than the total reported for the same period in 2020, while confirmed case volumes totalled more than 116,000 – 22% higher than in the first half of 2022.

"Fraud is a major problem here in the UK and issues such as our fast and efficient payments systems, high levels of digital adoption and the widespread use of the English language around the world are all likely playing a role in the rise of APP fraud," says Donald.

Big Tech and fraud

The world's largest tech companies, such as Apple, Google and Meta, have faced increasing calls to be held to the same regulatory standards as banks and fintechs, given their prominence in the payments landscape.

There is also growing evidence that social media platforms are a hotbed of scams and fraudulent activity.

Revolut conducted an analysis of its UK customer base and found that in 2023, 60% of reported scam cases originated from three major social media platforms: Facebook, Instagram and WhatsApp. Across the same period, 33% of the total value of all money lost to scams could be traced back to Meta platforms.

In 2022, according to the UK Finance Annual Fraud Report, 78% of APP fraud cases originated online and social media platforms accounted for the greatest number of online fraud cases, given that around three-quarters of online fraud starts on social media.

Some banks and consumers have begun calling for more action at government level, but also more transparency from the social media companies themselves.

Proprietary data from UK bank Barclays published in August 2023 revealed that 87% of all scams now take place on tech platforms, including social media, online marketplaces, and dating apps.

The bank's research found that 78% of consumers want technology companies to do more to prevent scams on their platforms, particularly as 76% reported feeling unsafe on social media as a direct result of the presence of scammers.

Donald adds: "The fact that currently these other sectors bear no responsibility for reimbursing victims means that there is little commercial incentive for them to truly tackle the problem that proliferates on their sites, platforms and networks. This needs to change.

"If we are to see a real difference, we need them to do more with us to protect consumers and share the burden of the fight against criminals."

The power of AI in fraud detection
As the tactics adopted by fraudsters become more sophisticated, organisations need to deploy increasingly advanced tools and solutions for truly effective monitoring of fraud.

For that reason, many organisations are now harnessing AI and machine learning in the fight against fraud. Generative AI's ability to scan many millions – even trillions – of data points in seconds and to identify anomalies is particularly useful for fraud detection and, therefore, prevention.

> "We expect to see a continued focus by criminals on trying to trick people into divulging their personal and financial information"
>
> **Andy Donald, director of communications, UK Finance**

Businesses have a need to protect their own reputations, of course, but they also need to offer their existing customers assurances that they are doing all they can to prevent fraudulent activity from occurring in the first place.

Money and reputation lost to fraud is extremely difficult, if not impossible, to claw back. More than half of respondents to KPMG's Global Banking Fraud Survey reported recovering less than 25% of fraud losses.

This is why investing technologies and tools that will prevent fraud from occurring in the first place is – or should be – top of mind for businesses in today's environment.

Earlier this year, UK-based fintech Revolut introduced a new scam detection feature which is powered

by AI. It works by assessing the likelihood that a customer is being prompted to make a card payment as part of a scam. In such cases, the feature effectively "interrupts" the scammer by declining the payment.

As with any fraud monitoring tools, it is a balancing act between accurately detecting and stopping fraud, and allowing customers to make genuine payments without excessive friction.

David Eborne, head of fraud at Revolut, said in a statement at the time that some banks are "increasingly restricting, or heavily limiting" the ability to make card payments to crypto and investment websites.

However, he added that Revolut's advanced fraud detection feature had been designed to "ensure that customers who want to perform legitimate payments continue to do so, but also intervene to protect those who are being guided by criminals to make fraudulent ones".

AI and machine learning are not a silver bullet, however. Riccardo Tordera-Ricchi, The Payments Association's head of policy and government relations has said it is watching the development of AI in the payments space closely and working with the industry to separate "genuine solutions from the hype".

"We have known for years that machine learning is the only thing with the sophistication and the capacity to tackle increasing volumes of fraud, but it's not a simple case of installing an AI solution and watching it clean up fraud on your system," Tordera-Ricchi adds.

Open Banking and fraud

Where does Open Banking sit within a broader conversation about fraud? Open Banking-enabled payments are known to be more secure than other payment methods.

However, while the ecosystem might recognise this, there is almost certainly an education piece required, to convey the message about Open Banking payments and security to individuals and businesses.

The banking industry seems torn as to the impact, positive or negative, on fraud. In its Global Banking Fraud Survey, KPMG reported that Open Banking is considered "a significant challenge" in fraud risk by banks, given that it requires opening up access to third-party data.

On the flip side, banks recognised the benefit from Open Banking of "a richer customer dataset" in helping them to identify and prevent fraudulent activity, according to the same survey.

What's next?

The Payment Systems Regulator is introducing a new reimbursement requirement, which is due to come into effect on 7 October this year. By making payment firms meet the cost of reimbursement, the PSR hopes to "incentivise the industry to further invest in end-to-end fraud prevention".

The PSR has stipulated that the maximum level of reimbursement per claim will be set at £415,000, in line with the maximum award the Financial Ombudsman Service can make when considering complaints.

> "Our fast and efficient payments systems, high levels of digital adoption... are all likely playing a role in the rise of APP fraud"
>
> **Andy Donald, director of communications, UK Finance**

This year also sees the expansion of CoP. Initially, the six largest banking groups were directed to implement the service. However, in October 2022, the PSR expanded the requirement to provide CoP to approximately 400 firms, which means that by October 2024, nearly all consumer payments will be covered by CoP.

UK Finance's Donald points out that, with the level of fraud in the UK having reached a point where it must be considered "a national security threat", international cooperation is "vitally important".

"Fraud is an ever evolving and complex threat to people and businesses. We also know that criminals change their tactics and try and circumvent security features," he says.

"We expect to see a continued focus by criminals on trying to trick people into divulging their personal and financial information," he says.

"The other issue we will need to contend with is the rapid pace of technological change and the greater prevalence of AI, which will continue to make the fight against fraud more challenging."

IN FOCUS

3.5m

The estimated number of incidents of fraud experienced by adults between April 2022 and March 2023

Source: Office for National Statistics

40%

Fraud accounts for more than 40% of crime in England and Wales

Source: National Crime Agency

13%

The percentage of fraud cases reported to Action Fraud or the police by victims

Source: Crime Survey of England and Wales

ENHANCING FRAUD PREVENTION STRATEGIES: THE VALUE OF INTEGRATED SOLUTIONS

Ruud Grotens
head of risk solutions consulting
Bottomline

WHY TRANSACTION MONITORING AND BEHAVIOURAL ANALYTICS EMERGE AS ESSENTIALS IN THE FIGHT AGAINST FRAUD

"Integrated fraud solutions bridge the gap between disparate types of fraud, recognising their interconnected nature"

In the fast-paced world of payments, fraud remains an ever-present threat, costing institutions and customers billions annually. To combat this pervasive issue, payment professionals are increasingly turning to integrated suites of fraud solutions, recognising the indispensable role they play in safeguarding transactions.

Among these solutions, transaction monitoring and behavioural analytics emerge as essentials, working in tandem with Verification of Payee systems and other fraud prevention measures to fortify defences.

Transaction monitoring acts as the vigilant detective of banking operations, meticulously scrutinising every transaction for signs of suspicious activity. By comparing current patterns with historical behaviour, Bottomline Secure Payments can swiftly detect anomalies and raise alerts, serving as an early warning system against potential fraud attempts. However, transaction monitoring alone may not capture all fraudulent activities, necessitating the augmentation of behavioural monitoring.

Behavioural monitoring delves deeper, analysing typical patterns of behaviour and activity to identify deviations or outliers. It serves as an initiative-taking measure, flagging unusual actions such as unauthorised account access, or atypical payment behaviour.

By combining transaction and behavioural monitoring, payment professionals can effectively detect and halt fraudulent activities in real-time – Bottomline's Secure Payments boasts an impressive average millisecond response time – mitigating potential losses and preserving trust.

Time is of the essence

According to data published by the UK's Payment Systems Regulator (see page 13), challenger banks are currently enabling the most APP fraud.

From that point of view, the urgency for adopting or improving payment fraud defences that can handle high volumes and stop fraud both in real-time, has never been greater.

Insider fraud, which is far too often underestimated, poses a significant threat to organisations. Collaborative efforts between internal bad actors and external criminals can result in APP fraud, through data leakage, consequential substantial financial losses and reputational damage, for example.

Integrated fraud solutions bridge the gap between disparate types of fraud, recognising their interconnected nature. Siloed approaches to fraud prevention overlook the critical linkages between insider fraud, and payment fraud, leaving organisations vulnerable to sophisticated schemes.

To combat evolving fraud tactics, an integrated approach to internal and external fraud prevention is imperative. The best integrated fraud prevention technology should offer out-of-the-box libraries with best practice fraud risk indicators that provide ongoing flexibility for comprehensive behavioural analytics, real-time alerting, and transaction blocking, allowing organisations to reduce risk, and prevent fraud loss.

By breaking down silos and adopting a unified perspective on fraud, organisations can enhance their resilience against emerging threats and safeguard their commercial interests.

Staying ahead

The battle against fraud is an ongoing endeavour, requiring constant vigilance and adaptation. Fraudsters continually innovate and exploit vulnerabilities, necessitating proactive measures and advanced analytics to stay one step ahead.

By embracing integrated internal and external fraud prevention strategies and fostering collaboration across different sectors, payment professionals can effectively mitigate risks and uphold the integrity of the financial system.

In conclusion, the value of integrated fraud solutions cannot be overstated. By combining transaction monitoring, behavioural analytics, and Verification of Payee systems, organisations can fortify their defences against internal and external fraud, and protect their assets.

Payments Orchestration, Messaging and Connectivity

Securely communicate financial transactions within and between financial institutions, globally and locally, while easily managing payment compliance, mitigating risk, and exceeding customer expectations.

bottomline.com

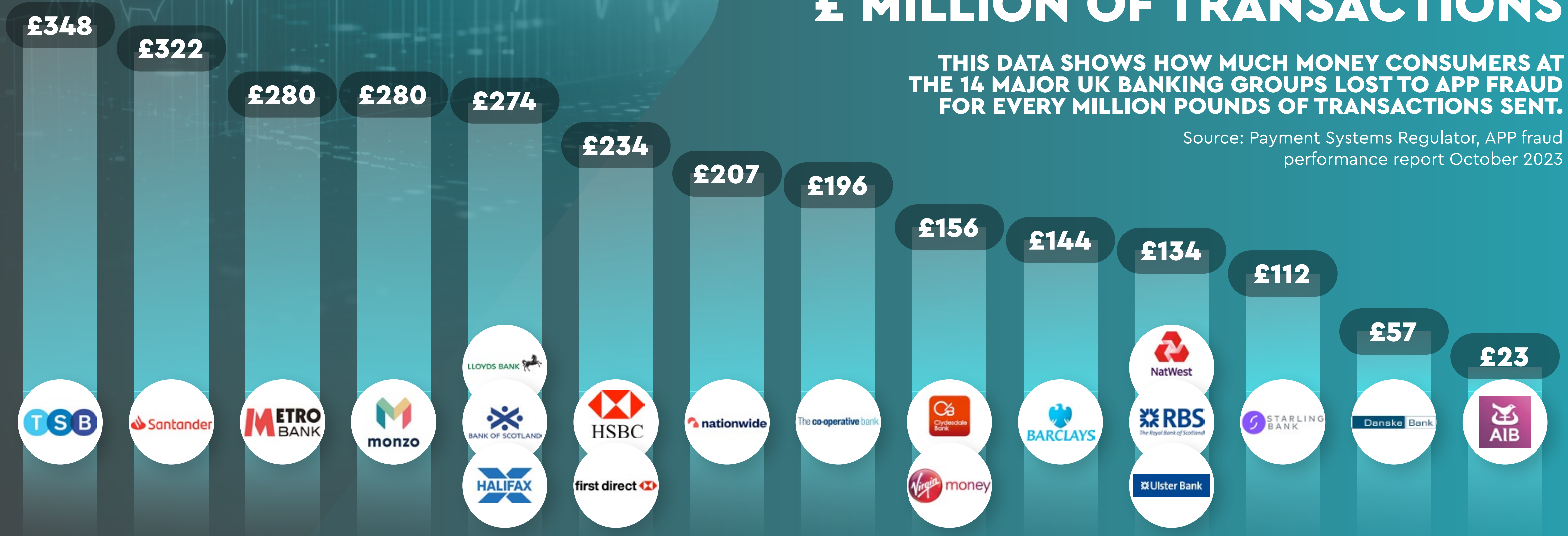
Accelerate Your Digital Payments Transformation Strategy Today!

IN FOCUS

VALUE OF APP FRAUD SENT PER £ MILLION OF TRANSACTIONS

THIS DATA SHOWS HOW MUCH MONEY CONSUMERS AT THE 14 MAJOR UK BANKING GROUPS LOST TO APP FRAUD FOR EVERY MILLION POUNDS OF TRANSACTIONS SENT.

Source: Payment Systems Regulator, APP fraud performance report October 2023



CONFIRMATION OF PAYEE: A CRUCIAL TOOL IN COMBATING APP FRAUD IN THE UK

Mark Bish
product lead risk solutions – corporates
Bottomline

Erez Nounou
product lead risk solutions – financial messaging
Bottomline

BOTTOMLINE'S MARK BISH AND EREZ NOUNOU ASSESS THE BENEFITS AND LIMITATIONS OF CONFIRMATION OF PAYEE, AND CONSIDER HOW ITS SCOPE CAN BE EXPANDED

The UK's Confirmation of Payee (CoP) initiative, aimed at validating bank account ownership, has emerged as a pivotal tool in the fight against Authorised Push Payments (APP) fraud in the UK.

By October 2023, CoP had achieved 99% coverage of GBP accounts addressable by Faster Payments and has already shown promising results, with a 17% reduction in APP fraud in 2023. However, compared to initiatives like the IBAN name-check in the Netherlands, which achieved an 81% reduction in fraud within foreign domestic transfers, CoP's impact might seem less impressive.

Expanding CoP

One of the key lessons learned from CoP implementation is the necessity of a holistic approach to fraud prevention.

Focusing solely on APP fraud leaves other payment types vulnerable to exploitation – for instance, direct debits. While the CoP use case has been extended to allow use of the service to verify payers when creating new DDIs, the lack of a formal mandate for use, as given for APP, leaves consumers and businesses susceptible to fraudulent activity. Extending CoP to encompass direct debits could provide a comprehensive solution to mitigate fraud across various payment methods.

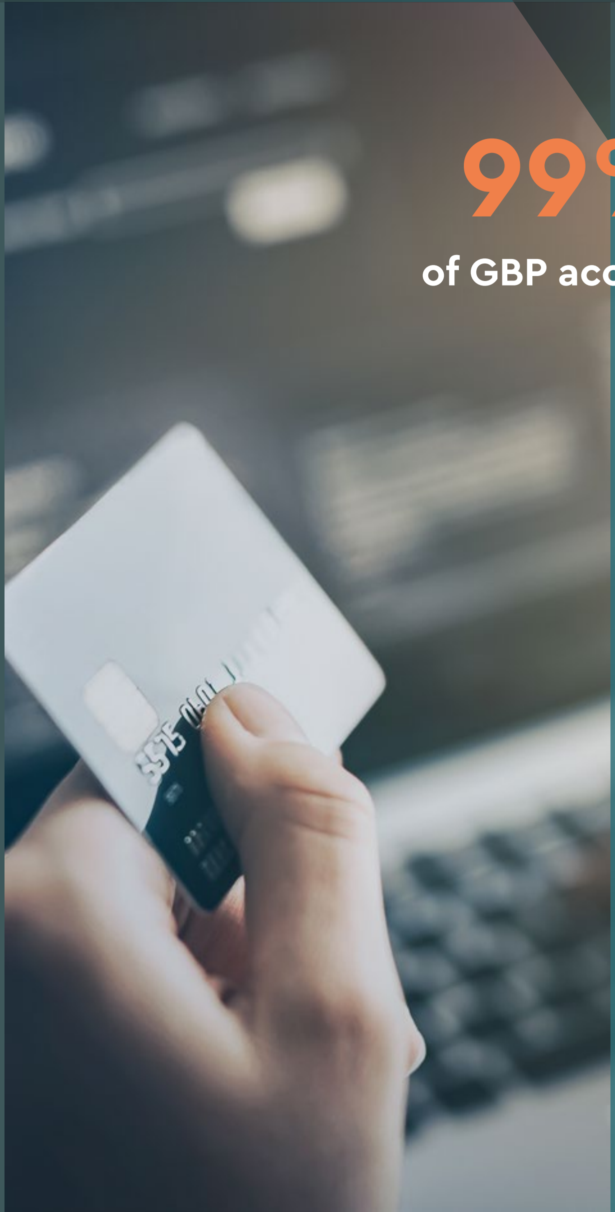
Looking to the future, there is a growing consensus on the need to expand CoP beyond bank-to-bank transfers, with a clear need to drive

ubiquity of use for all direct debits and direct credit payments, and explore its application to digital wallets and credit cards, which could address existing gaps in fraud prevention.

While credit card schemes offer some protection against fraudulent transactions, the inability to confirm the account holder's name leaves a significant vulnerability. Introducing a CoP-like mechanism for credit cards could enhance security and bolster consumer trust.

Limitations of CoP

Despite its efficacy, CoP is not without its shortcomings. The system's flexibility, while advantageous in accommodating minor errors like 'fat fingers,' also opens the door to potential abuse. Distinguishing between accidental errors and malicious intent remains a challenge, highlighting the need for additional layers of protection or AI-driven tools to discern intent accurately.



By October 2023, CoP had achieved **99% coverage** of GBP accounts addressable by Faster Payments

Moreover, the current payload of CoP queries is insufficient, lacking crucial contextual information that would enable easier detection of suspicious activity and allow for a more nuanced response.

Providing additional information, including who is making the request, their account details, the purpose of the request and the associated risk or value, strengthens fraud detection efforts by allowing the recipient to include these details as part of their risk assessment, vary flexibility in matching logic and temper the answer they return.

By enhancing CoP's capabilities to include this information, recipients are better able to make more informed decisions regarding transaction legitimacy, protect themselves from indemnity claims, and provide the sender with a response that offers greater protection for them and their customers. This is particularly important with the introduction of mandatory reimbursement for APP fraud.

Collaboration is key

As the financial landscape evolves, collaboration between stakeholders becomes paramount. Payment service providers (PSPs), regulators, and solution providers must work together to streamline CoP implementation and address emerging challenges. Bottomline, for instance, offers comprehensive fraud prevention solutions that complement CoP, providing support throughout the transaction journey.

Looking ahead, the expansion of CoP presents a significant opportunity for the UK payments sector. By broadening eligibility criteria and introducing new technical models, CoP aims to enhance coverage and effectiveness in combating fraud. The next stage must be to mandate CoP for corporates for all payment channels to further drive down payment fraud.

However, for mandated PSPs, the priority must be CoP integration, leveraging resources and guidance provided by regulatory bodies and solution providers.

In conclusion, CoP represents a crucial step forward in fraud prevention within the UK payments sector. By addressing its limitations, expanding its scope, and fostering collaboration, CoP has the potential to revolutionise payment security, ensuring a safer and more reliable financial environment for all stakeholders.

"Looking ahead, the trajectory of fraud prevention hinges on global collaboration and regulatory alignment"

SAFEGUARDING PAYMENTS: LESSONS LEARNED FROM CONFIRMATION OF PAYEE

Mark Bish
product lead risk solutions – corporates
Bottomline

Erez Nounou
product lead risk solutions – financial messaging
Bottomline

HOW EFFECTIVE IS CONFIRMATION OF PAYEE AT TACKLING APP FRAUD AND HOW DOES IT WORK ALONGSIDE OTHER FRAUD PREVENTION SOLUTIONS?

In the relentless battle against authorised push payments (APP) fraud, the UK has spearheaded efforts to fortify its payment verification systems, with Confirmation of Payee (CoP) emerging as a pivotal tool. However, as financial institutions seek to stem the tide of fraud, not only domestically but also globally, it is crucial to extract key lessons from CoP implementation and augment existing processes.

Hailed as a pre-verification mechanism, CoP scrutinises payee details to thwart inadvertent errors in transaction inputs. Yet, as the landscape of fraud evolves, there's merit in considering an additional layer: verifying the payer. This proactive approach aims to identify anomalous behaviours, such as unauthorised individuals initiating large transactions, thus fortifying defences against insider threats.

Taking an holistic approach

Transaction and behavioural monitoring, synergistically integrated with Verification of Payee, furnish a holistic fraud mitigation strategy. By flagging suspicious activities—like unusual transaction volumes or unfamiliar beneficiaries—these mechanisms pre-empt potential fraud attempts, mitigating risks in real-time.

However, the efficacy of CoP is tempered by the constraints of legacy infrastructure, which remains a bastion for fraudsters seeking vulnerabilities. Institutions tethered to archaic systems face mounting pressure to fortify defences amid escalating threats. Patching vulnerabilities and system upgrades, albeit essential, present logistical and financial hurdles, underscoring the imperative for concerted investments in modernisation.

Furthermore, the advent of real-time payments has become a double-edged sword, offering unparalleled convenience but also fertile ground for fraudsters. The urgency to scrutinise transactions within milliseconds underscores the need for swift, adaptive fraud prevention solutions.

As the UK seeks to continue to mitigate APP fraud, the discourse has shifted from CoP to a broader narrative of fraud prevention. Mandatory reimbursement provisions incentivise payment service providers to embrace comprehensive fraud mitigation measures, encompassing CoP alongside other fraud checks, like sanction screening and behavioural monitoring. However, the limited information provided within the current payload for CoP queries makes it difficult for recipients to make more informed decisions regarding transaction legitimacy when responding to CoP queries, and to protect themselves from mandatory reimbursement claims that they could otherwise have blocked.

Looking ahead, the trajectory of fraud prevention hinges on global collaboration and regulatory alignment. Will mandatory reimbursement schemes and extended validation windows, pioneered in the UK, find resonance internationally? We suspect so, in light of the expansion of CoP-like mandates in Europe and beyond. The impetus lies in transcending geographical boundaries to forge a unified front against fraud.

In closing, CoP serves as a cornerstone in fraud prevention, but its efficacy is magnified when integrated into a multifaceted approach. By fortifying legacy systems, embracing real-time analytics, and fostering regulatory convergence, the financial ecosystem can strengthen its defences against the ever-evolving spectre of fraud.

ADVANCING GLOBAL FRAUD PREVENTION: ROLLING OUT VERIFICATION OF PAYEE

Frédéric Viard
head of commercial product management – financial messaging
Bottomline

Erez Nounou
product lead risk solutions – financial messaging
Bottomline

IN THE GLOBAL FIGHT AGAINST FRAUD, THE UK'S EXPERIENCE PROVIDES VALUABLE LESSONS

In the landscape of global payment systems, the UK has emerged as a pioneer in combatting fraud, particularly with its innovative tool Confirmation of Payee (CoP).

As payment professionals worldwide seek to bolster their fraud prevention strategies, the UK's experience provides invaluable insights and lessons for extending verification of payee solutions, like CoP, globally.

Addressing misconceptions

The notion of 'Faster Payments, Faster Fraud' is a common misconception, often rooted in the irrevocable nature of instant payments. Frédéric Viard, Head of Commercial Product Management – Financial Messaging at Bottomline, rightly points out that instant payments, once initiated, cannot be easily recalled or cancelled, leaving little time for verification.

However, Erez Nounou, Product Lead – Risk Solutions, Financial Messaging at Bottomline, emphasises that the speed of transactions does not inherently make them more vulnerable to fraud; rather, it is the lack of opportunity for pre-validation checks. This is something that will be remedied as part of the SEPA Inst mandate in Europe.

Value of pre-verification and fraud checks

Pre-verification tools like CoP, Bank Account Verification (BAV) and Verification of Payee are pivotal in preventing fraudulent transactions. Nounou highlights that pre-validation allows for upfront checks on payee details, providing a layer of protection before funds are transferred.

Additionally, regular fraud checks are essential for maintaining payment hygiene and detecting fraudulent patterns.

Standardisation and interoperability

While different countries may implement similar verification schemes, achieving interoperability remains a challenge. Viard emphasises the need for a common rulebook, or standard, to ensure consistency across borders.

Achieving interoperability would enable seamless communication between different payment systems and enhance global fraud prevention efforts.

SEPA Inst: The challenges and opportunities

The SEPA Inst mandate presents both challenges and opportunities for European banks and financial institutions (FIs). Viard underscores the importance of determining the model for implementing Verification of Payee at a cross-border level, ensuring efficient and secure payment processing within the EU.

Leveraging ISO 20022 for enhanced fraud mitigation

The adoption of the ISO 20022 standard brings enhanced data structuring, reducing room for error and improving fraud detection accuracy. Structured data enables more focused fraud checks, reducing false positives and enhancing overall efficiency in fraud mitigation efforts.

Toward a global framework for fraud prevention

As the global payments landscape evolves, there is a growing need for a unified approach to fraud prevention. While challenges persist, such as standardisation and interoperability, lessons from the UK's experience with CoP offer a roadmap for payment professionals worldwide.

By embracing pre-verification tools, leveraging standardised frameworks like ISO 20022, and fostering collaboration, the industry can work towards a global standard for mitigating fraud and ensuring secure payment ecosystems.

"The fight against fraud requires better collaboration and knowledge sharing between everyone in the payments system"

APP FRAUD: COP AND THE FIGHT AGAINST FRAUD

Kate Frankish
chief business development officer
and anti-fraud lead
Pay.UK

PAY.UK'S KATE FRANKISH EXPLAINS HOW COP IS HELPING IN THE FIGHT AGAINST APP FRAUD AND THE IMPORTANCE OF FRAUD PREVENTION STRATEGIES

CoP has completed a milestone

2bn checks

We operate in an industry which is fast-paced and constantly evolving, and fraud is, unfortunately, a modern-day reality.

We launched Confirmation of Payee (CoP) in 2020 as a layer of good friction to help protect banking customers from misdirected payments and certain types of fraud.

The service helps UK banks, building societies and other payment services providers (PSPs) to mitigate Authorised Push Payment (APP) fraud by providing a platform for PSPs to warn payers in situations when the payee name, sort code and account number entered by the payer does not match that which is registered.

We recently announced that since launch, CoP has completed a milestone two billion checks, and on average, checks for more than 1.9 million payments every day are carried out. The value of CoP as a tool in the fight against fraud is undeniable, as highlighted by the widespread adoption of the service.

CoP currently covers over 92% of Faster Payments transactions, with more than 100 organisations now using the service. This is set to grow further, as the PSR has mandated around 400 organisations to implement the service by October 2024, following the success of the service.

More, however, needs to be done. Fraudsters move fast and adapt quickly, coming up with novel methods and using technology to their advantage.

Harnessing AI to tackle emerging threats

Many types of fraud, particularly romance and investment scams, entail extensive social engineering and manipulation of the victim. This has a devastating emotional and financial toll, and this is one of the key reasons why tackling this growing criminal threat is a top priority for both Pay.UK and the wider industry.

The application of Artificial Intelligence (AI) in the financial sector has brought about a paradigm shift in fraud prevention strategies. By analysing vast volumes of data, AI models can recognise patterns that indicate fraudulent activities, enabling banks to adapt to emerging threats and intervene in real-time.

Pay.UK has a dedicated fraud prevention programme which is exploring multiple and complementary services to help our customers reduce both fraud and friction. This includes leveraging better, and more effective, use of data for detection and prevention to equip the industry with tools to enable them to intervene proactively before it affects people.

When a fraud does occur, financial protection is an important right, and we are working to ensure that innocent victims are reimbursed consistently through the implementation of the APP scam reimbursement policy.

The fight against fraud requires better collaboration and knowledge sharing between everyone in the payments system: the government, regulators, banks, social media companies and law enforcement.

Isolated solutions are no longer enough. The key to effective fraud prevention lies in fostering a united front against this ever-growing and ever-evolving issue.

Bottomline™

Transforming the Way Businesses Pay and Get Paid

800,000+
Businesses Using Bottomline

$10 Trillion
Payments Moved Annually

Top 3
Swift Service Provider

Bottomline.com

OPEN
BANKING
EXPO

Ground Floor
Cromwell House
15 Andover Road
Winchester SO23 7BT

+44 (0)207 993 5159
www.openbankingexpo.com
hello@openbankingexpo.com

X @OpenBankingExpo
in Open Banking Expo

IN ASSOCIATION WITH

Bottomline