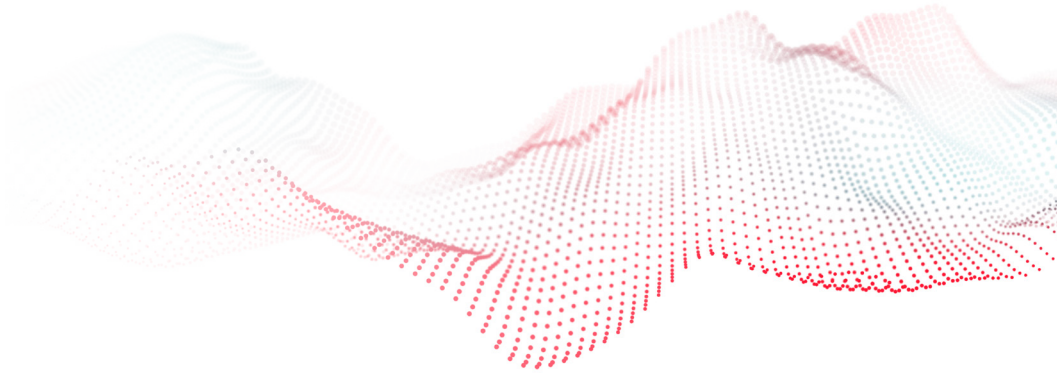
ThreatMark

→ WHITEPAPER

THE LIABILITY SHIFT

The context of fraud losses responsibility and mitigation.



Contents

Executive Summary

This whitepaper examines the state of the electronic payments market and the changes in liability for fraud losses being introduced by regulators across the globe.

It aims to provide financial sector executives with the background to the liability changes and to offer solutions to effectively prevent fraud and reduce the negative impact that the liability changes may have on banks and payment service providers (PSPs).

The electronic payments industry is developing dynamically. Current data shows that by 2030, the global market will grow at a CAGR of 14–15%.[4,5] This is due to post-COVID changes in consumer behavior, the popularity and ease of electronic payments, but also modern technologies (instant payments) and frameworks (open banking) that allow new players to enter the market. However, the development of non-cash payments has resulted in increasing incidents of fraud, the majority of which are caused by scams. The increase is so high that some have referred to it as a 'scampocalypse'.

These dynamic changes are leading national regulators, as well as the industry players themselves, to rethink their existing fraud liability practices. While the burden of loss has historically rested on the fraud victims, we are now seeing an increasing shift of responsibility to the financial institutions that send or receive the funds.

The liability shift serves to better protect consumers who are vulnerable to the advanced tactics of fraudsters. At the same time, however, it inevitably places a higher burden on banks and payment service providers. For them, liability shift means higher prevention and liability costs, compliance and regulatory challenges, and the necessary investment in technology.

One way financial institutions can effectively combat advanced fraudster tactics while maintaining a seamless customer experience is through the use of behavioral intelligence. Compared to traditional fraud detection systems, this technology offers effectiveness against new types of fraud such as Authorized Push Payment (APP) scams, fast implementation, and reduced user authentication expenses. In the context of the upcoming liability shift, behavioral intelligence will help reduce the damage that fraud causes to banks and payment service providers, not only on compensation costs but also on customer trust.

1. Introduction

Definition and background

To understand the context of payment fraud and the associated liability shift, it is necessary to be aware of the current situation in the sector of electronic payments and its recent developments.

Among the most important aspects that have affected the electronic payments market recently are:

- Instant payment systems
- Open banking frameworks
- FinTech market growth
- Changes in consumer habits caused by COVID-19

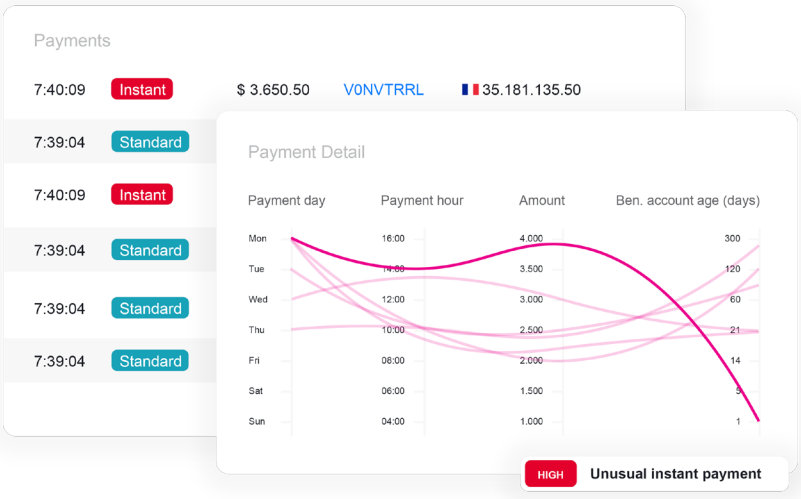
Instant Payment Systems

The payment sector has been considerably affected by the global adoption of instant (also called real-time) payment systems, revolutionizing the way transactions are conducted.

Instant payment systems are electronic payment platforms that enable immediate transfer of funds between bank accounts or financial institutions. Unlike traditional payment methods, such as credit card transactions or bank transfers that may take several days to process, instant payment systems facilitate near-instantaneous transactions, often completed within seconds or minutes.

The implications are profound. Instant payment systems (such as SEPA Instant Credit Transfer in the EU, Faster Payments in the UK, or the recently introduced FedNow in the USA) significantly boosted payment speed and convenience, overall customer experience, economic activity, and industry innovation and competition.

Data shows that by 2027, the number of instant payment transactions will exceed 376 billion globally, which is a 289% growth in comparison to 97 billion in 2022.[1]



Open Banking Frameworks

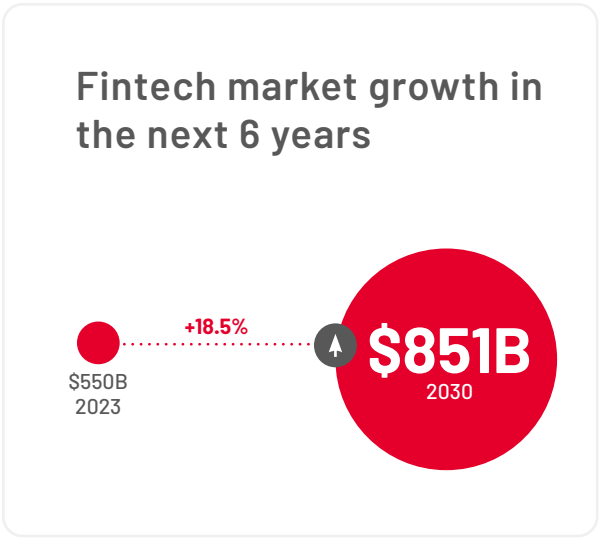
Instant payment systems are not the only driver of the electronic payments market. Open banking frameworks cannot be omitted as they create a system that provides third-party access to financial data using application programming interfaces (APIs). Using APIs, banks can transform their core systems to innovate and integrate with internal systems and external partners in an easier, more secure, and controlled way.

One of the earliest and most notable instances of an open banking framework emerged with the implementation of the Revised Payment Services Directive (PSD2), introduced by the European Union in 2018.

Societal Changes Related to COVID-19

Finally, the current developments of the electronic payments market are an echo of the COVID pandemic, during which people abandoned the use of cash for fear of contagion, but also because they simply did not have the opportunity to use it.

At a time when consumers were confined to their homes during quarantines and lockdowns, cashless payments proved to be the ideal solution and often the only option for making transactions.



FinTech Market Growth

Instant payment systems and open banking frameworks have, among other factors, played a significant role in the current FinTech boom.

As of July 2023, publicly traded FinTech companies represented a market capitalization of $550 billion, a doubling from 2019. Over the same period, there were more than 272 fintech unicorns, with a combined valuation of $936 billion. That's a seven-fold increase from 39 firms valued at $1 billion or more five years ago[2]. Data also suggests that by 2030, the FinTech market will be worth $851 billion and will grow at an 18.5% CAGR between 2023 and 2030[3].

GlobalData states the global digital payments market will be valued at a total of $2,476.8 trillion in 2023, and is expected to grow at a CAGR of 14.3% by 2030[4].

Global Context

According to Capgemini's World Payment Report 2023 (aptly titled Where is the cash?), the amount of non-cash transactions will reach nearly 1.3 trillion in 2023 and 2.3 trillion by 2027, which would be double the amount in 2022. Capgemini expects that volume growth will continue accelerating at a 15% CAGR from 2022 to 2027[5].

Electronic payments are a vital part of the economy of the European Union. In 2021, the value of non-cash transactions in the EU was €240 trillion, while back in 2017 it was €184.2 trillion. Both the value and quantity of European cashless transactions are increasing[6].

In North America, non-cash payment volumes are expected to rise at a 6.5% CAGR over the period 2022–2027.[5] Growth in the region is supported by the fact that the US Federal Reserve launched FedNow Service in July 2023, aiming to create a real-time payments network similar to that in Europe.[7] FedNow complements Clearing House's RTP service (launched in 2017), however, both services support push payments only. It is important to note that a new open banking framework and rules are being developed by the US Consumer Financial Protection Bureau[8] and Canada has as well announced plans to launch open banking in 2023.

2. Understanding the Fraud Landscape

Emerging Threats

Alongside technology, market, and regulatory changes, however, fraudsters are not falling behind. Advances in speed, availability, and ease of electronic payments have introduced new risks and vulnerabilities, such as limited verification time, irreversibility, or lack of transaction context. This makes them attractive to fraudsters, especially when it comes to scams and social engineering. New forms of fraud, such as authorized push payment fraud (APP fraud), take advantage of instant payment technologies.

The generative artificial intelligence and its current proliferation also bring both benefits and new threats. For example, the European Police Office (Europol) recently mentioned that the emergence of large-scale artificial intelligence language models may contribute to fraud.[9]

> *"ChatGPT's ability to draft highly realistic text makes it a useful tool for phishing purposes. The ability of LLMs to re-produce language patterns can be used to impersonate the style of speech of specific individuals or groups. This capability can be abused at scale to mislead potential victims into placing their trust in the hands of criminal actors."*
>
> Europol

Data on Fraud

An increasing number of online payment frauds can be observed worldwide.

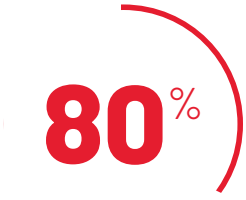
- According to **Europol**, online fraudsters generate billions of euros in illicit profit every year and represent a major crime threat.[10] Euro Retails Payment Board (ERPB) findings assert that the scale of fraud cases and loss is likely to grow over the coming years due to professionalized crime, the modernization of fraud techniques (i.e. use of AI), continued digitization of society, and the rise of instant payments.[11]
- In the **USA**, consumers reported losing nearly $8.8 billion to fraud in 2022, an increase of more than 30 percent over the previous year.[13]
- In the **UK**, unauthorized fraud losses across payment cards, remote banking, and cheques reached £726.9 million in 2022.[14] APP frauds accounted for £485.2 million.
- The latest Targeting Scams report, published by the **Australian** Competition & Consumer Commission, has revealed Australians lost a record $3.1 billion to scams in 2022.[15]
- The **APAC** region is no exception in the increasing number of frauds. Singapore is a typical example: In the first half of 2023, the number of scams and cybercrime cases increased by almost 70% compared to the same period in the previous year. More than 91% of these cases were scams. The total losses amounted to $334.5 million (January–June 2023).[16] Across the APAC region, scams account for 54% of all digital banking fraud.[17]

APP Fraud on the Rise

The data shows that an increasing portion of fraud now accounts for authorized push payment fraud. APP fraud is the act of manipulating victims into making real-time payments to fraudsters, typically by social engineering attacks involving impersonation. However, there are two basic types of these scams[18]:

- Malicious payee: e.g., tricking someone into purchasing goods that don't exist (or are never received).
- Malicious redirection: e.g., a fraudster impersonating bank staff to get someone to transfer funds out of their bank account and into that of a fraudster.

In the United Kingdom, APP fraud accounted for 40% of fraud losses in 2022.[19] In the first half of 2023, £239.3 million was lost to APP fraud.[13] According to a report jointly published by ACI Worldwide, a provider of payment software, and GlobalData, it is projected that APP fraud losses will see a twofold increase in the United Kingdom, India, and the United States by 2026.



of reported UK fraud started online in 2022.

These losses are estimated to reach $5.25 billion (£4.44 billion), with a compound annual growth rate of 21% over the specified period.[19]

Other Industry-Specific Risks

As digital developments continue at a rapid pace around the world, fraudsters are less constrained by geography, and the threat of new types of fraud can spread unrestricted across countries and continents. In addition, the banking and financial sector faces different specific fraud risks due to the nature of its operations, the value of the assets involved, and the sensitivity of financial transactions.

Different types of fraud can fall under different objectives, whether it is money theft, identity theft, or other objectives. The channels that fraudsters use also vary, from SMS, and phone calls to emails to the increasingly common social networking sites. **Almost 80% of reported APP fraud cases in the UK in 2022 started online.**[13] Some industry-specific fraud risks include:

- Payment card fraud
- Account takeover (ATO)
- Phishing, vishing, and social engineering
- Identity theft
- Money laundering
- Cybersecurity breaches etc.

3. Compliance and Regulatory Considerations

Global Standards

Global standards regarding online fraud or scam reimbursement vary across regions and countries, as each jurisdiction may have its own regulations and guidelines addressing consumer protection, financial transactions, and fraud liability. Consumer protection laws, liability frameworks, regulatory guidance, and voluntary codes of conduct differ significantly from one country to another.

Who Carries the Cost of Fraud?

The losses caused by fraud are currently almost exclusively on the shoulders of the defrauded consumer. If banks are responsive to their customers and have the resources to address losses that fraud caused them, they do it as a customer service, not by default. The approach to refund is usually based customer's actions and the so-called gross negligence principle.

This means that if it is proven that the customer has violated basic caution rules (for example, by passing on authentication data to a stranger), they lose their right to compensation. The outcome of the reimbursement process also depends to a large extent on whether the customer seeks legal advice.

For this reason, the level of compensation and overall approach varies across countries, banks, and payment solution providers. A great example of inconsistency is the UK's Payment Systems Regulator data from 2022, which shows that in the UK alone the percentage of refunded losses from APP fraud (by volume) ranges from 6% to 94% across individual financial institutions.[20]

However, current trends and the changing approach of regulators show that this is slowly but surely shifting.

Upcoming Regulatory Changes

Regulators are now changing their approach, prioritizing consumer protection and shifting accountability of fraud to the financial institutions and payment companies. This shift of liability in this context refers to the change in responsibility for covering losses due to a fraudulent transaction, which can be observed throughout every continent.

The UK as Early Adopters

One of the countries leading the way is the UK. The Payment Systems Regulator (PSR) released new guidelines coming into effect in 2024, which requires sending and receiving banks to be equally liable for customer reimbursement for fraudulent transactions. Customers will be protected under consistent minimum standards, with all victims who report APP fraud being compensated within five working days and vulnerable customers being offered additional protection.

By releasing new guidelines, PSR aims to extend the existing Contingent Reimbursement Model (CRM) Code released in 2019. While in the 2019 version, the equal sharing of liability for damages is voluntary, in the new proposal it is an industry requirement.

Changes will also affect the operator of Faster Payments, Pay.UK, which will need to put in place an effective monitoring regime to ensure PSPs follow the reimbursement requirements. The changes to the rules will also apply within the Faster Payment system, as unfortunately, the payment speed advances both the volume and success of APP scams.

New guidelines set an important benchmark by reinforcing the principle of protecting and compensating victims of APP scams and also encouraging financial institutions to adopt more effective and powerful safeguards.

Greece Follow Closely Behind

Greece has recently joined the liability shift, compensating victims of payment fraud if the amount exceeds €1,000. Law 5019/2023 (in effect from September 2023) aims to increase the security of online payment transactions and protect customers from fraudulent activities.[21]

Norway, Sweden, and Denmark have also made similar changes in legislation.[22]

The European Union

The EU has already announced a planned revision of its Second Payment Services Directive (PSD2). The planned legislation changes – PSD3 and the new Payment Services Regulation (PSR1) – will be far-reaching and significantly affect liability for fraud.

PSD3 and PSR1 introduces a framework to help banks and payment service providers fight fraud. However, the EU legislation will also support victims of fraud by giving them the right to reimbursement by their bank/PSP under specific circumstances.

For example, when the consumer falls victim to "spoofing" (a scam where the fraudster pretends to be an employee of the consumer's bank), or when the IBAN/name verification service fails to detect a mismatch between the name and IBAN of the payee.

USA

In the United States, some local players are already partially adjusting the rules for compensating customers who fall victim to fraud.[23] One example is the payment app Zelle, which, under pressure from US lawmakers and the Consumer Financial Protection Bureau, has begun compensating its customers who have fallen victim to fraud.

To put this in perspective, it is estimated that in 2021 alone, customers of this app lost $440 million to all types of fraud.[24] Zelle did not disclose details of its new policy, allegedly out of concern over false compensation claims.

What it Means for Banks and PSPs

Financial institutions and PSPs need to prepare themselves to be obliged to actively prevent fraud and to share in the losses caused by successful fraudsters in the future, which can have several significant effects. These effects can vary based on the specific liability-shifting measures and regulations in place, but some common impacts include:

Financial Impact

Financial institutions and PSPs may face direct financial losses due to their increased responsibility in preventing fraud. This includes higher demands for financial compensation to customers, as well as increased costs related to implementing more stringent security measures and investing in advanced fraud detection technologies.

Brand and Recognition in Market

Brand value heavily relies on trust. By securing a safe and trustworthy financial environment for their customers and streamlining compensation processes, banks will have the opportunity to gain significant reputational points. Fraud compensation options that go even beyond regulatory obligations will become an important competitive advantage for banks and payment service providers.

Compliance and Regulatory Challenges

Banks will need to invest in compliance measures to meet new regulatory standards. Increased liability may lead to monitoring obligations, which means a higher administrative burden. Adjusting systems, protocols, and processes to comply with the new regulations around fraud prevention and liability sharing can also be costly.

Technological Investments

Banks may need to invest in cutting-edge technologies, such as biometric authentication, multi-factor authentication, or behavioral intelligence, to enhance security and reduce fraud risks.

4. Strategies for Effective Fraud Prevention

Challenges of Fighting Fraud

Banks and PSPs play a key role in the fight against online payment fraud. To strengthen their defenses, protect consumers, and preserve the integrity of financial ecosystems, financial organizations need to employ multifaceted strategies. As the online payment fraud landscape is constantly evolving, it presents a dynamic challenge that requires adaptive and innovative approaches.

The situation is not made easier by the fact that the type of fraud hardest to detect is experiencing the greatest growth: APP fraud. The intricacy of APP fraud lies primarily in the fact that traditional banking fraud detection and safeguarding often fail here. Given the technological and, unfortunately, tactical sophistication of the manipulations used by fraudsters, it is relatively easy for ordinary users to fall victim to such an attack. Since it is then the authorized user themselves who makes the payment, it is very difficult for financial institutions to detect and prevent this kind of fraud.

The Need for New Measures

Addressing APP fraud in the context of instant payment systems requires a multi-layered approach. Robust fraud prevention measures, real-time transaction monitoring, enhanced customer education, improved authentication methods, and collaboration among financial institutions and regulatory bodies may mitigate risks and protect consumers and businesses from falling victim to such scams.

To avoid losing the trust of their customers and the threat of large financial losses, financial institutions will have to introduce new methods and technologies to detect advanced types of fraud. However, investing additional extensive resources in technology and fraud prevention may be a challenge. According to a recent Capgemini report, banks must deal with the fact that they are losing out on former revenue sources as the payment ecosystem and customer habits change.[5]

On the other hand, increased cost sensitivity may motivate banks to avoid fraud losses that they would have to reimburse to their customers due to the liability shift.

> *"Payment executives surveyed in this report indicate that nearly 80% of traditional payment revenue sources (fee, fund, and float income) are stressed. In parallel, costs related to regulatory compliance, scheme implementation (including ISO20022 and SWIFT gpi), and payments modernization leave limited resources to invest in innovation."*
> **Capgemini's World Payments Report 2023**

5. The role of ThreatMark

Risk Mitigation with Behavioral Intelligence

One way to detect all types of fraud, even if it is APP fraud perpetrated by the legitimate owner of the account, is to use behavioral intelligence. The key to the success of behavioral intelligence lies in the combination of behavioral biometrics (which can reliably detect whether a legitimate user is making an account transaction) and behavioral analytics (which can detect unprecedented anomalies in a user's behavior that would indicate that a legitimate user is acting under the influence of fraudsters).

Behavioral biometrics leverages the fact that every user is unique. This applies to several online behavioral metrics:

- Mouse movements
- Keystroke dynamics
- Phone swipes
- Touch events
- Additional phone sensors and session data

Behavioral biometrics is therefore a powerful identity affirmation tool that can reliably detect whether an account transaction is being made by a legitimate user. Similarly, each user has certain patterns of behavior regarding their transactions and routine actions on their account.

Behavioral intelligence can recognize when the individual deviates from normal behavior – for example, under pressure from APP fraud.

Whether it's an unusual typing rhythm, segmented typing, suspicious mouse polling rates, active ongoing phone calls, or other red flags, behavioral analytics can catch even small deviations from usual behavior and stop APP fraud as it happens – all in real-time.

For these reasons, behavioral intelligence plays a crucial role in combating various types of online payment fraud – including APP scams – due to its ability to provide dynamic and context-aware insights into user behavior.

When behavioral intelligence is combined with other anti-fraud technologies across the entire customer journey, a very efficient yet cost-effective solution is the result.

ThreatMark's Platform offers a comprehensive solution that analyses users at every step of their online journey, from banking login to transactions, across all digital channels.

ThreatMark's Behavioral Intelligence is:

Comprehensive

To achieve truly comprehensive protection using behavioral intelligence, ThreatMark leverages an AI-powered behavior profiling engine and utilizes a combination of device, threat, user identity, and payment information. This leads to a 70% better detection rate over traditional FDS.[25]

Always Up-To-Date

By using machine learning, the solution is always up-to-date and not at risk of becoming obsolete like rule-based systems. Artificial intelligence can swiftly adapt to new fraudulent scenarios that rules cannot support.

Easily Integrated

ThreatMark's Behavioral Intelligence is easy to deploy, offering both cloud and on-premise solutions. Test driving and launching behavioral intelligence takes just a few weeks, sometimes days.

Frictionless

Trust is important, but so is convenience. ThreatMark's Behavioral Intelligence lowers false positives by up to 90%.[24] Higher detection reliability improves the customer experience and paves the way for customer retention and revenue growth.

Value of Behavioral Intelligence in Liability

For banks and payment service providers, the liability shift inevitably means an even greater emphasis on scam prevention and protection against fraud losses. Leveraging technology solutions based on behavioral intelligence – such as ThreatMark's – will help banks meet regulatory requirements while adding value. Moreover, its implementation is very fast and cost-effective, so even resource-constrained organizations can benefit from this solution.

Data shows that implementing Behavioral Intelligence brings significant cost reduction as it eliminates false positives and decreases authentication costs by 90% (such as SMS costs) in comparison to traditional FDS.[24]

As a result, leveraging behavioral intelligence allows help banks and PSPs:

- **Safeguard** their customers' financial assets
- **Protect** their reputation and avoid customer churn
- **Reduce** overhead costs associated with fraud investigations and remediations
- **Uphold** confidence in their organization and in the financial system at large

Conclusion

Today's global landscape shows us that modern cashless payments are becoming increasingly popular with consumers and in the B2B sector.

However, to make further growth of electronic payments possible, it will be necessary to make the industry more secure. This is because the growing appetite and success of fraudsters can erode the most important asset – consumer trust, the fundamental premise of the entire digital payment industry. In this context, the liability shift is a step in the right direction. It will help to maintain the confidence of bank and PSP customers that they are protected from fraudsters.

For banks and PSPs, the situation is more complex. It turns out that to keep up with fraudsters (and preferably outpace them), informing and educating customers is not enough. It will be necessary to leverage the latest technologies.

One such technology proving to be effective against modern fraud attempts such as APP fraud is behavioral intelligence. Its power lies in its ability to detect suspicious behavior by the user themselves acting under the influence of the fraudster. At the same time, implementing behavioral intelligence is relatively easy, cost-effective, and delivers fast results.

Behavioral intelligence can protect customers and financial institutions from fraudster attacks swiftly, efficiently, and in real-time. Many legacy approaches to fraud security lag in this context. It is truer than ever that the way you fight fraud matters.

Explore ThreatMark's Behavioral Intelligence Platform here

Glossary

APP scam/fraud Authorized push payment scam/fraud – a type of fraud where individuals are deceived into authorizing the transfer of funds from their own account to a scammer's account.

Authorized payment A transaction that has been approved and validated by the account holder or an authorized party to transfer funds or payment from their account.

Behavioral analytics A broader spectrum of data analysis to understand and identify patterns in user behavior. It involves the collection, monitoring, and analysis of various behavioral data points.

Behavioral biometrics An analysis of unique patterns in an individual's behavior to authenticate their identity.

Behavioral intelligence Behavioral intelligence refers to the process of gathering, analyzing, and interpreting data related to human behavior to derive insights, patterns, and predictive models. Such data is proving to be a vital tool in the fight against fraudsters.

CRM Contingent Reimbursement Model – a framework designed to offer protection and reimbursement to victims of authorized push payment (APP) scams in the United Kingdom.

FDS Fraud detection system

FinTech Financial Technology – firms using new technology to compete with traditional financial methods in delivering financial services.

Gross negligence A heightened degree of negligence representing an extreme departure from the ordinary standard of care.

Phishing An attempt to obtain sensitive data through a fraudulent request in an email or on a website, where the perpetrator pretends to be a legitimate company or reputable person.

PSD2 Revised Payment Services Directive – a European law that governs payment systems in the European Union.

PSD3 A last revision of the Payment Services Directive that regulates electronic payments and the banking ecosystem within the EU.

PSP Payment service provider

PSR1 Payment Services Regulation – a new EU regulation to replace PSD2. PSR1 aims to create a more harmonized market for payment services with significantly fewer differences and inequalities between member states.

PSR Payment Systems Regulator – the UK's independent economic regulator of payments systems.

Scam A fraudulent activity designed to manipulate victims into willingly providing their money, sensitive information, or valuables under false pretenses.

Social engineering Psychological manipulation of people to force them to perform actions or divulge confidential information.

Spoofing An act of disguising a communication from an unknown, usually fraudulent source as being from a known, trusted source.

Unauthorized payment A transaction made from an account without the explicit approval, consent, or authorization of the account holder or an authorized party.

Vishing The fraudulent practice of making or leaving voicemail messages posing as phone calls from reputable companies to trick individuals into disclosing personal information such as bank details and credit card numbers.

References

[1] "Instant Payments: Future Opportunities, Regional Analysis & Market Forecasts 2022-2027. Juniper Research. December 5, 2022. https://www.juniperresearch.com/research/fintech-payments/emerging-payments/instant-payments-research-report/.

[2] "Fintechs: A New Paradigm of Growth." McKinsey & Company. October 23, 2023. www.mckinsey.com/industries/financial-services/our-insights/fintechs-a-new-paradigm-of-growth#/.

[3] "FinTech Market - Forecast(2023 - 2028)." IndustryARC. 2023. https://www.industryarc.com/Report/18381/fintech-market.html.

[4] "Digital Payments Market Size, Share, Trends and Analysis by Region, Mode of Payment, Industry and Segment Forecast to 2030." GlobalData. May 5, 2023. https://www.globaldata.com/store/report/digital-payments-market-analysis/.

[5] "World Payments Report 2023." Capgemini. September 14, 2023. https://www.capgemini.com/insights/research-library/world-payments-report/.

[6] "Electronic Payments in the EU." European Commission. June 2023. https://finance.ec.europa.eu/system/files/2023-06/230628-payments-fida-factsheet_en.pdf.

[7] "Federal Reserve Announces that Its New System for Instant Payments, the FedNow® Service, Is now Live." Board of Governors of the Federal Reserve System. July 20, 2023. https://www.federalreserve.gov/newsevents/pressreleases/other20230720a.htm.

[8] "Laying the Foundation for Open Banking in the United States." Consumer Financial Protection Bureau. June 12, 2023. https://www.consumerfinance.gov/about-us/blog/laying-the-foundation-for-open-banking-in-the-united-states/.

[9] "The Criminal Use of ChatGPT – a Cautionary Tale about Large Language Models." Europol. March 27, 2023. https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models.

[10] "Online Fraud Schemes: A Web of Deceit." Europol & IOCTA. December 20, 2023. https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf.

[11] "ERPB working group on fraud interim findings." Euro Retail Payments Board, November 20, 2023. https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/20th-ERPB-meeting/ERPB_Working_Group_on_fraud_Interim_findings.pdf.

[12] "New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022." Federal Trade Commission. February 23, 2023. https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022.

[13] "Over £1.2 Billion Stolen through Fraud in 2022, with Nearly 80 per Cent of APP Fraud Cases Starting Online." UK Finance. May 11, 2023. https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app.

[14] "Targeting Scams: Report of the ACCC on Scams Activity 2022." Australian Competition & Consumer Commission. April 17, 2023. https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2022.

[14] "MID-YEAR SCAMS AND CYBERCRIME STATISTICS 2023." Singapore Police Force. September 13, 2023. https://www.police.gov.sg/-/media/9B26F6C9613B4760AC78D15EBCDB4048.ashx.

[15] "2023 APAC Digital Banking Fraud Trends Report." BioCatch. June 28, 2023. https://www.biocatch.com/resources/white-paper/digital-banking-fraud-trends-apac-2023.

[16] "APP Scams." Payment Systems Regulator. October 2023. https://www.psr.org.uk/our-work/app-scams/.

[17] "Growth in APP Scams Expected To Double by 2026 – Report by ACI Worldwide and GlobalData." ACI Worldwide. November 15, 2022. https://investor.aciworldwide.com/news-releases/news-release-details/growth-app-scams-expected-double-2026-report-aci-worldwide-and.

[18] "APP fraud performance report." PSR. October 2023. https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/.

[19] "Greece – New Rules for the Protection of Consumers from Online Fraud ("Phishing")." Ernst & Young. March 3, 2023. https://www.ey.com/en_gr/tax/tax-alerts/greece-new-rules-for-the-protection-of-consumers-from-online-fraud-03-2023.

[20] "The Nordic Bank'S Authorized Push Payment Fraud Guide." Feedzai. December 9, 2022. https://feedzai.com/blog/the-nordic-banks-authorized-push-payment-fraud-guide/.

[21] "Banks in Talks to Reimburse Zelle Customers Who Were Scammed." Wall Street Journal. December 5, 2022. https://www.wsj.com/podcasts/your-money-matters/banks-in-talks-to-reimburse-zelle-customers-who-were-scammed/a8f3fca7-4ba2-4f28-84a4-3a3add380332.

[22] "Payments app Zelle begins refunds for imposter scams after Washington pressure." Reuters. November 13, 2023. https://www.reuters.com/technology/cybersecurity/payments-app-zelle-begins-refunds-imposter-scams-after-washington-pressure-2023-11-13/.

[23] "Anti-Fraud Suite." ThreatMark. 2022. https://www.threatmark.com/dist/files/ThreatMark-AFS-Datasheet.pdf.

ThreatMark is dedicated to fostering trust in the digital world by protecting individuals from fraud and securing their personal information. We do this by deploying cutting-edge Behavioral Intelligence solutions that help financial institutions and fintechs detect and defend against fraud attacks before they happen.

ThreatMark harnesses the untapped potential of behavioral data and user-device interactions to proactively identify and thwart fraud attacks, offering financial entities a robust, forward-thinking line of defense against evolving scams. By collaborating closely with our partners, we not only assist them in combatting fraud but also significantly reduce false positives of existing fraud controls. As a result, we help financial institutions and fintechs lower operational costs and pave the way for customer retention and revenue growth.

Learn more at **threatmark.com**.

ThreatMark