JAYWING

Strengthening financial crime defences

A PSP's guide to fighting financial crime

Introduction

It’s clear that Payment Service Providers (PSPs) are facing major challenges in the fight against financial crime.

As digital payments surge and transaction speeds accelerate, money launderers are finding increasingly sophisticated ways to exploit PSP systems—and the numbers paint a concerning picture. In 2023, UK customers suffered nearly £1.2 billion in financial crime losses, with a significant portion flowing through payment service channels.

This creates a perfect storm for PSPs, who must process high volumes of instant payments while managing multiple payment methods—from traditional bank transfers to digital wallets and cryptocurrencies. Each new payment option becomes another potential route for financial crime to enter the system. Take Authorised Push Payment (APP) fraud, which accounted for £580 million in losses during the first half of 2023 alone.

With 77% of these scams originating online, these fraudulent transactions often mark just the beginning of complex money laundering schemes.

Regulators have noticed this trend and are demanding better defences. The EU’s 6th Anti-Money Laundering Directive (6AMLD) and strengthened UK requirements now require PSPs to implement enhanced due diligence, robust verification processes, and sophisticated transaction monitoring.

In this guide, we’ll cover:

- Why traditional AML approaches no longer work
- Five new challenges PSPs face in AML compliance
- Building stronger AML defences: Best practices for PSPs
- Real-world AML case study

£1.2b

lost to financial crime in the UK (2023)

£580m

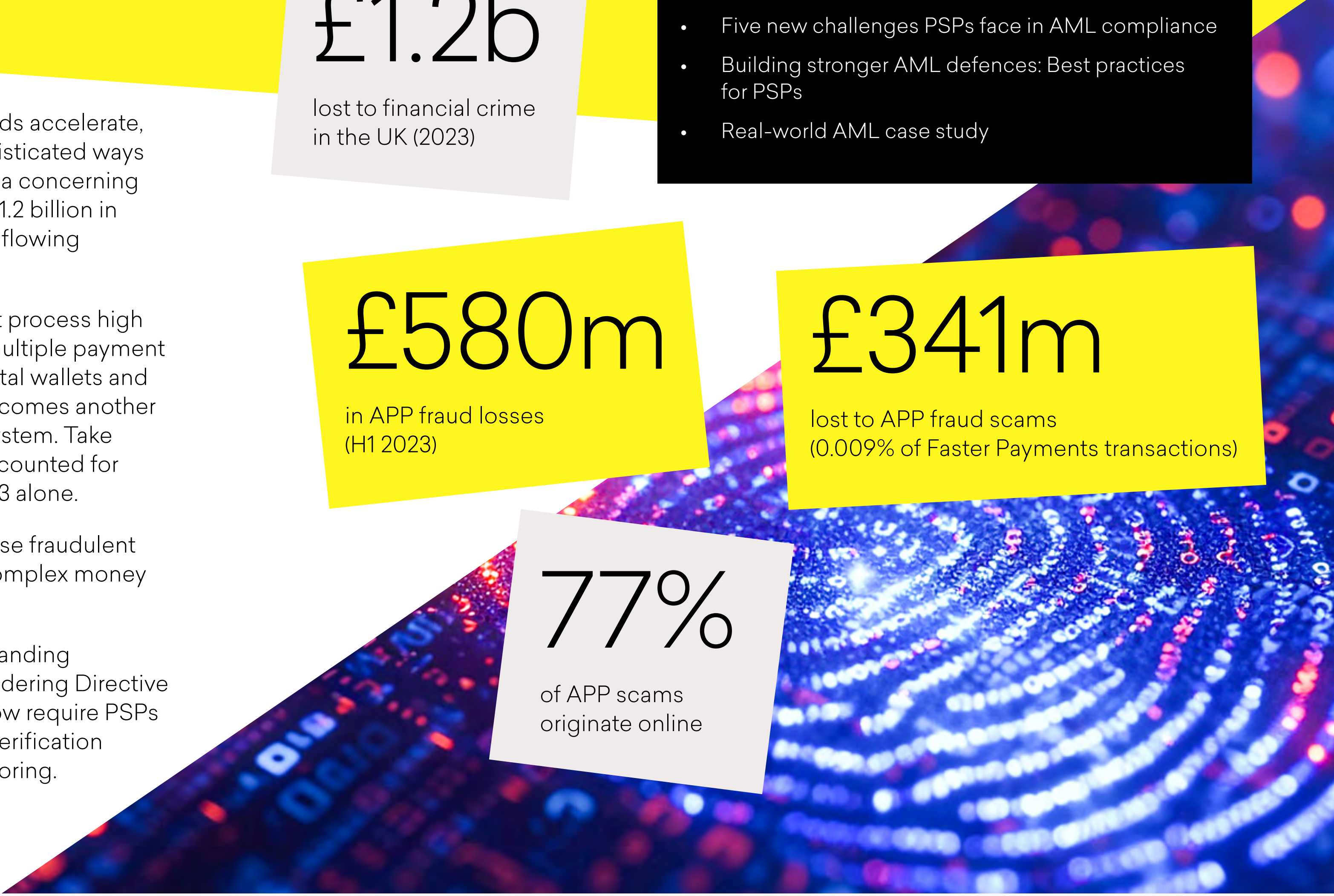
in APP fraud losses (H1 2023)

£341m

lost to APP fraud scams (0.009% of Faster Payments transactions)

77%

of APP scams originate online



Why traditional AML approaches are no longer enough

Traditional AML systems were built for a time when payments were simpler, and criminals were less organised.

Static rules and manual reviews could raise obvious red flags, but payments are now far more complex. Advanced tactics, like professional mule networks and blended payment methods, are designed to exploit the gaps in these rigid frameworks.

These systems also fall short when it comes to new payment methods, such as cryptocurrencies and digital wallets. The rise of e-wallets has brought new vulnerabilities, with hacking incidents increasing as fraudsters explore alternative approaches. While social engineering remains their primary method, these attacks are becoming more sophisticated, particularly in Europe.

Without the flexibility to track these channels, PSPs are left exposed to evolving risks. Add to that the inefficiency of high false positive rates—wasting resources and frustrating customers—and it's clear that outdated approaches can no longer keep pace.

With financial criminals growing more sophisticated and payment methods more diverse, PSPs need AML strategies that can adapt, scale, and respond in real-time. Anything less puts compliance, reputation, and customer trust at risk.

Next: Key challenges for PSPs

Five new challenges PSPs face in AML compliance

1 Regulatory pressure

The regulatory landscape for PSPs continues to tighten, with frameworks like **6AMLD** and **PSD2** creating new compliance challenges. These changes demand hefty operational adjustments from PSPs, particularly in their approach to financial crime prevention.

Regulators now expect PSPs to demonstrate proactive crime prevention measures, moving beyond simple after-the-fact detection. This requires sophisticated systems that can identify and stop suspicious activities before they become problematic.

The stakes are higher than ever, with regulatory bodies implementing stricter penalties for non-compliance. Of course, PSPs also face the additional challenge of balancing these security requirements with open banking initiatives, which require seamless integration with external systems.

Each new regulation adds another layer of complexity to PSP operations. The pressure to adapt quickly is constant, yet existing systems and processes can't be neglected. Beyond the immediate impact of fines, PSPs who fail to meet these standards risk serious damage to their reputation and customer trust.

Real-time transaction monitoring has become essential as payments flow through multiple providers simultaneously. PSPs must track and analyse these transactions instantly, while maintaining complete visibility across their networks.

Five new challenges PSPs face in AML compliance

As of 2024, cross-border e-commerce accounts for approximately **31.2% of all global online sales**, with the market valued at an estimated £1.6 trillion. By 2028, cross-border transactions will likely constitute up to **33% of global e-commerce**.

In the United Kingdom, cross-border online shopping is notably prevalent. A 2024 survey found that **52% of UK consumers had purchased from international online retailers in the past year**.

2 Cross-border complexity

If you're operating internationally, things get even trickier. What's flagged as suspicious in one country could be ignored in another. This inconsistency can cause headaches for compliance teams.

Legal requirements vary significantly between regions, making it nearly impossible to implement standardised compliance processes. Some jurisdictions demand extensive due diligence and frequent reporting, while others maintain more relaxed standards.

This regulatory variation creates a delicate balancing act for PSPs. For instance, actions taken to ensure compliance in one market might inadvertently breach regulations in another. PSPs must carefully navigate these differences to avoid service disruptions or restrictions that could impact their operations.

The key to managing these challenges lies in implementing flexible compliance systems. These systems need to adapt to regional requirements while maintaining comprehensive oversight of global operations.

You know what makes this especially challenging? A mistake in cross-border compliance doesn't just affect operations – it can seriously damage a PSP's reputation and trustworthiness in multiple markets.

Five new challenges PSPs face in AML compliance

3 Real-time payments

The rise of real-time payments has revolutionised financial transactions, but it's also created new vulnerabilities in AML compliance. Criminal organisations can now transfer illicit funds across borders within milliseconds, outpacing traditional monitoring systems.

This shift in transaction speed demands sophisticated AML strategies from Payment Service Providers. Systems must now detect and flag suspicious activity instantly – even a few seconds' delay could mean the difference between stopping criminal activity and losing track of funds completely.

The challenge isn't just about speed. Transaction volumes continue to grow exponentially, requiring systems that can scale effectively without compromising accuracy or creating processing delays. PSPs need solutions that can handle millions of transactions while maintaining precision in fraud detection.

E-commerce transactions are growing at **twice the rate** of PoS. And global real-time transactions will reach more than **575 billion** by 2028.

Criminal tactics are constantly evolving, making system adaptability crucial. Systems that can't keep pace with new criminal strategies risk exposing significant vulnerabilities in their defences.

The consequences of inadequate real-time monitoring extend far beyond immediate financial losses and regulatory penalties. Recent cases (see right) have shown how negative media coverage of AML failures can inflict lasting damage on a PSP's reputation and market position.

Spotlight: Banks in the news

TD Bank's record penalty:

In October 2024, TD Bank faced over $3 billion in fines from U.S. authorities for failing to prevent money laundering activities linked to drug trafficking and terrorism. The bank admitted to significant lapses in its AML program, leading to a cap on its U.S. asset growth and the resignation of its CEO.

Starling Bank's AML Failures:

In October 2024, Starling Bank was fined £28.96 million by the FCA for AML failings, including opening 54,000 high-risk accounts and lapses in sanctions screening. The deficiencies exposed the bank to misuse by criminals and sanctioned entities.

Five new challenges PSPs face in AML compliance

4 Professional mule networks

Money laundering has reached new levels of sophistication, with criminal networks leveraging mule accounts distributed across multiple countries and PSPs. This makes traditional detection methods increasingly ineffective.

The challenge is compounded when criminals mix different payment methods – traditional bank transfers, prepaid cards, and cryptocurrencies – creating a complex web of transactions that's difficult to track. These operations often move faster than traditional detection systems can analyse, leaving significant gaps in AML defences.

It's also crucial to consider the role of recipient banks and PSPs in the equation. Liability is increasingly being shared, meaning AML and fraud checks must account for both incoming and outgoing funds. Without this dual focus, PSPs risk exposing their systems to further vulnerabilities.

Traditional rule-based systems simply can't keep up with these advanced tactics. PSPs must adopt advanced analytics and AI-powered models capable of processing vast amounts of data in real-time. These tools can detect subtle patterns and anomalies, flagging suspicious activities before they escalate into full-scale financial crimes.

It's not just professional networks driving this problem. Younger people, including children, are being coerced or incentivised to allow their accounts to be used by mules. This often ties into wider issues of trafficking and financial exploitation, with devastating consequences.

In 2023, UK Finance reported a 60% rise in cases involving under-21s acting as money mules, highlighting the urgency of addressing this growing issue.

Five new challenges PSPs face in AML compliance

5 Customer experience vs compliance

Nobody likes a clunky payment process. But with rising fraud risks, PSPs need to keep payments secure without driving customers away. It's a tough balance, and the challenges show up in two key areas:

False positives

False positives present a significant business challenge when legitimate transactions trigger suspicious activity alerts. These unnecessary flags can seriously impact customer relationships and business growth. Customers who face repeated transaction delays often look for alternative providers, while lengthy verification processes can put off potential new customers.

Security vs speed

The tension between security and speed creates another challenge. Today's customers expect instant payments, but each additional security measure adds friction to the process.

Lengthy verification steps during onboarding can lead to abandoned applications, while strict transaction controls might limit a business's ability to expand into new markets.

Payment speed is key in markets where real-time transactions are standard practice. Even a slight delay in processing can push customers toward competitors who offer faster services.

Key takeaway

PSPs need to find innovative ways to strengthen security without compromising on transaction speed. The solution lies in implementing intelligent systems that can accurately distinguish between genuine and suspicious activity.

And on top of this, there's still the data challenge...

The data challenge

At the heart of these problems is **data quality**. Good data is critical for effective compliance and fraud prevention, but PSPs often find themselves dealing with.

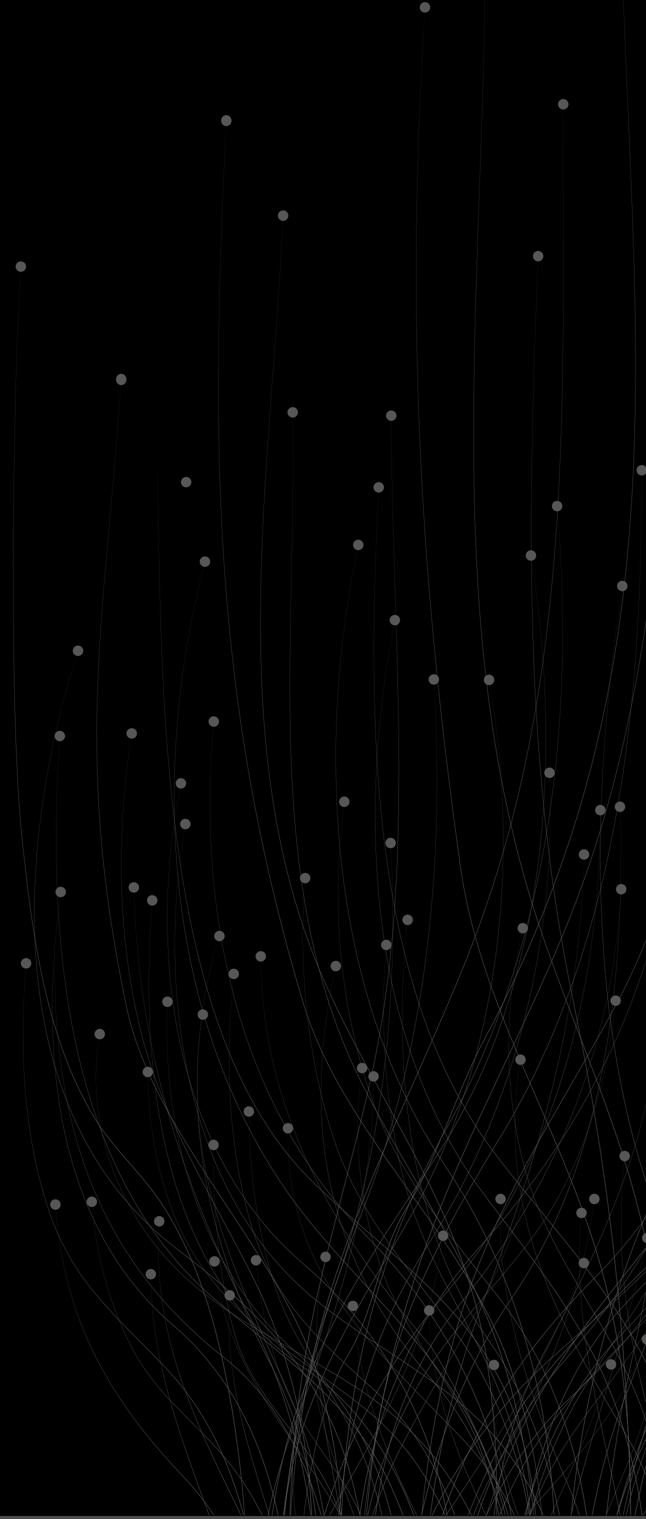
Data-driven decisions drive business growth in several ways:

- **Incomplete information:** Missing customer details or device identifiers make it hard to spot risks.
- **Siloed systems:** Data spread across different platforms creates blind spots.
- **Slow data feeds:** Delayed updates mean slower detection of suspicious activity.
- **A baffling array of external data sources:** PSPs must evaluate and understand numerous options to optimise their fraud defences effectively.

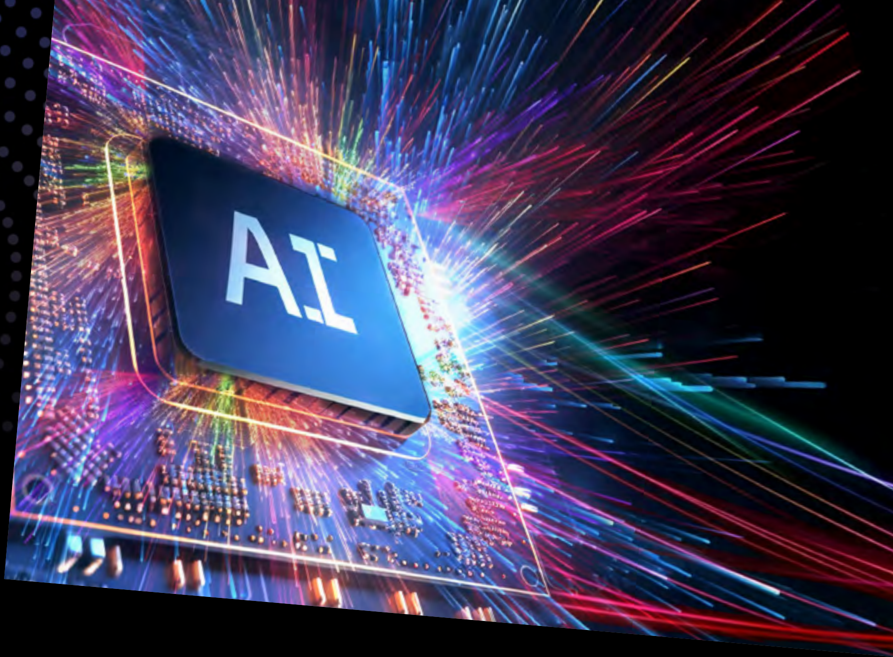
Fixing these issues means breaking down silos, integrating data in real-time, and using advanced analytics to turn raw information into actionable insights.

Side note: Data management is another area we specialise in at Jaywing (more on this here).

In summary:
By tackling these challenges head-on, PSPs can create a smoother experience for customers while staying on top of compliance demands.



Building stronger AML defences: Best practices for PSPs



With transaction volumes rising and financial criminals becoming more sophisticated, PSPs need best practices that combine cutting-edge technology with strategic collaboration.

Here's how PSPs can build smarter, more effective AML defences:

Embrace AI, Machine Learning, and advanced techniques

Artificial intelligence (AI) and machine learning (ML) are transforming AML by moving beyond static rule-based systems. Combined with other essential strategies, they provide a proactive and adaptable approach to tackling financial crime.

Key practices include:

- **Graph databases:** Track payments and identify links to uncover money mule networks and suspicious activity.
- **Profiling for pattern detection:** Analyse transaction-level behaviours to spot subtle anomalies.
- **Application screening and onboarding:** Strengthen processes beyond the minimum requirements to stop fraudulent accounts before they're created.
- **Positive friction:** Introduce slight delays in payments to give customers time to pause and recognise potential risks.
- **AI-powered insights:** Detect emerging threats in real-time and reduce false positives for a smoother customer experience.

Jaywing's AI-powered software – **Archetype** – helps PSPs take these capabilities further. Designed for speed, precision, and transparency, Archetype uses explainable AI to build advanced predictive models that spot risks and patterns with exceptional accuracy.

It enables compliance teams to act quickly, confidently, and effectively while seamlessly integrating into existing processes.

By adopting Archetype and these practices, PSPs can enhance their AML strategies, stay ahead of financial criminals, and maintain customer trust.

Federated learning: Bridging privacy and collaboration

Collaboration is key to tackling financial crime at scale, but sharing data across institutions often raises privacy concerns. Federated learning offers a solution by enabling organisations to share insights without exposing sensitive customer information.

- **Privacy-preserving insights:** Federated models work locally on data, combining results without revealing the underlying information.
- **Detecting networked risks:** From coordinated mule accounts to cross-border laundering schemes, federated learning uncovers patterns that span institutions.

This innovative approach ensures PSPs can work together to strengthen AML efforts while remaining compliant with stringent data protection laws like GDPR.

Balance security and customer experience

AML defences shouldn't come at the cost of customer satisfaction. Striking the right balance ensures your platform stays secure without frustrating legitimate users.

Best practices include:

- **Tailored risk controls:** Use AI to assess transactions based on individual risk profiles, reducing unnecessary blocks or delays.
- **Streamlined verification:** Optimise onboarding and authentication processes to minimise friction for low-risk customers.
- **Educating customers:** Companies have a responsibility to educate both their customers and staff about fraud, money laundering, and money mules.

The last point should be a major priority for firms. Customers should be empowered to recognise scams, while staff—especially call operators—need training to spot signs of duress or coercion, such as a customer being on another line. By equipping all parties with the right knowledge, businesses can reduce risks and improve their overall defences.

The right balance builds trust, improves retention, and ensures compliance efforts support—not hinder—business growth.

Leverage real-time capabilities

With instant payments now the norm, PSPs need AML systems that can match the speed and scale of today's transactions. Real-time capabilities are non-negotiable for spotting suspicious activity before funds vanish.

Focus on systems that:

- **Monitor transactions in real-time:** Flag and analyse high-risk payments instantly.
- **Scale seamlessly:** Handle surging volumes without losing accuracy.
- **Adapt continuously:** Learn from new data to stay ahead of evolving criminal tactics.

Failing to invest in real-time solutions can leave PSPs exposed to both financial and reputational risks.

Stay one step ahead with innovation

Financial crime is always changing, and AML frameworks must evolve alongside it. Emerging technologies offer PSPs exciting new ways to enhance their defences. Here are some trends we'd expect market leaders to adopt:

Best practices include:

- **Self-adaptive AI models:** These systems evolve automatically, adapting to new laundering techniques without manual updates.
- **Natural Language Processing (NLP):** NLP deciphers large volumes of unstructured data, like transaction narratives, uncovering risks that were previously impossible to detect.
- **Predictive analytics:** Advanced forecasting tools allow PSPs to anticipate vulnerabilities and act before they escalate.

By investing in future-facing solutions, PSPs can transform compliance from a regulatory burden into a competitive advantage.

Strengthening AML for today and tomorrow

The fight against financial crime has changed dramatically, and traditional AML approaches simply can't keep up. Today's PSPs face sophisticated mule networks, complex cross-border transactions, and the lightning speed of real-time payments. That's why new strategies are essential — ones that bring together smart technology, streamlined processes, and excellent customer experience.

With the right tools in place—from AI analytics and real-time monitoring to secure data sharing—PSPs can build stronger defences against financial crime while keeping payments flowing smoothly for their customers.

Ready to strengthen your AML defences?

Let Jaywing help you lead the way

Building a resilient AML framework doesn't have to be overwhelming. At Jaywing, we combine advanced analytics, AI-powered models, and deep industry expertise to help PSPs strengthen their defences.

From self-adaptive AI to predictive analytics, our tailored support ensures you're ready for whatever comes next.

Take the next step with confidence. Contact us to learn how we can help you build smarter AML defences.