UK Appoints Its First Fraud Minister — A Critical Turning Point in the Fight Against Financial Crime

Financial fraud has become one of the UK's most damaging, persistent, and underestimated national threats. The appointment of the UK's first Fraud Minister marks a decisive moment—one that could, if executed effectively, reshape the country's economic resilience, restore its global leadership in financial services, and provide meaningful protection for citizens targeted by increasingly sophisticated digital criminal networks.

At the Financial 360 Conference, Rt Hon Lord David Hanson delivered a direct and energising overview of the government's approach. His message was unequivocal: the UK cannot afford incrementalism. Fraud is not simply a crime problem; it is a strategic, systemic, macro-economic challenge affecting public trust, global competitiveness, and the stability of the digital economy.

Supported by Andrei Skorogatov of the Home Office—who outlined global payment fraud trends and the realities of cross-border criminal operations—Hanson's address signalled the first credible attempt in years to bring coherence to a fragmented landscape. For the first time, the UK is treating fraud prevention as a national strategy rather than a collection of isolated industry efforts.

---

1. Fraud in 2025: A Crisis of Scale, Speed, and Visibility

Fraud has evolved at a pace most regulatory systems, law-enforcement structures, and financial institutions have failed to match. What was once a niche financial crime has grown into a mass-market, industrialised criminal economy capable of inflicting systemic harm. Understanding the urgency behind the appointment of a 'Fraud Minister' requires recognising the scale of the problem.

Over the last decade, fraud losses in the UK have **doubled**, and the number of cases has **tripled**. In just the first half of 2025, **£629 million** was stolen across **2.1 million** reported cases. For any UK adult over the age of 19, the risk of experiencing digital fraud now stands at approximately **7.5% per year**. Scams occur once or twice every second.

This escalation reflects wider global trends. The EU recorded **€4.3 billion** in payment fraud losses in 2024. The United States reported a **72% increase** in fraud attacks and a **21% surge** in online fraud activity. Data from the Global Anti-Scam Alliance (GASA) and the OECD indicate that Asia-Pacific has seen explosive growth in cross-border investment scams, mule networks, and AI-assisted social engineering attacks.

The fraud economy has industrialised. Criminal groups operate across continents, routing money through crypto wallets, digital payment apps, and global mule networks at near-instant speeds. Fraud has become a scalable digital enterprise.

The takeaway is clear: fraud is not merely a policing issue. It is a national infrastructure vulnerability. It undermines confidence in digital payments, erodes trust in institutions, and threatens the UK's position as a global leader in financial services.

---

2. The Hidden Weak Link: Data Sharing and Institutional Resistance

Despite years of technical progress and investment in fraud tools, the UK's single greatest barrier to effective fraud prevention remains its longstanding inability—or unwillingness—to share data across institutions in real time. This structural issue has allowed criminals to exploit gaps that should have been closed a decade ago.

A striking example comes from the 2015 Digital Policy Alliance (DPA) initiative. Working with FIS Global and VocaLink (now Mastercard), the team analysed a single day of Faster Payments across several major banks. The results were remarkable: **75% of fraud could be stopped immediately** if banks shared key indicators. They also uncovered **eight mule networks** in a single day's data. The evidence was clear: cross-institution data sharing

works. Earl of Errol, DPA, presented the findings at the Worshipful Company of IT to a packed group of colleagues from across society and was well received.

Yet the project was halted. Banks and PSPs were unwilling to share information with their competitors. A supervised fraud hub was proposed but rejected. The institutional incentives—protect reputation, avoid liability, safeguard competitive advantage—overpowered the collective need to protect the public.

Other nations have faced the same challenges but pushed ahead with reform. Thailand introduced a Royal Decree enabling regulated real-time data sharing, reducing scam volumes. Singapore created a national Scam Surveillance Centre to integrate intelligence from banks, telecoms, and online platforms. Australia established the National Anti-Scam Centre to coordinate data flow across industries. The EU is embedding AI-driven fraud detection into the emerging Digital Euro infrastructure.

Meanwhile, the UK—an early leader in payments innovation—has fallen behind.

For the 'Fraud Minister' to deliver system-wide change, dismantling institutional resistance to data sharing must be a priority. Without real-time intelligence exchange, the UK will continue to fight a digital arms race with analogue coordination.

---

3. Regulatory Momentum: Stablecoins, Identity Verification, and the Coming Wave of Instant Payments

Regulatory reform often moves slowly, but in the financial crime domain it can also act as a powerful catalyst. The UK is now at a critical regulatory crossroads, where decisions around digital payments, identity verification, and stablecoins will shape fraud prevention for the next decade.

New legislation governing fiat-backed stablecoins introduces a requirement for continuous monitoring of KYC and AML data. Identity data can no longer remain static; risk profiles must adapt to real-time behavioural signals. This reflects how money moves today and how fraud operates—dynamically, instantly, and often across borders.

Similarly, the modernisation of **Confirmation of Payee (CoP)** may finally close an exploited vulnerability. For years, scammers relied on the fact that bank transfers did not require the real account owner's name to match the stated payee. This allowed criminals to impersonate institutions like HMRC or banks simply by typing a legitimate-sounding name into the payee field. With CoP 2.0, banks must verify the legal account owner's identity before approving payments, and this requirement will likely extend to international transfers such as SWIFT IBAN transactions.

Across the Channel, the EU's Instant Payments Regulation is reshaping the payment landscape more aggressively. By 2027, instant payments will be mandatory across the bloc. The EU is investing heavily in compliance automation, sanctions checking, fraud detection, and AI-driven transaction monitoring. Early contracts worth €79 million have been awarded to design systems that embed resilience, privacy, and security into the architecture of the Digital Euro.

The UK risks falling behind if its own systems do not keep pace. Regulatory divergence cannot become a competitive disadvantage.

Regulatory shifts alone will not eliminate fraud. But they establish stronger standards, push institutions toward continuous monitoring, and force alignment across borders. For the Fraud Minister, these reforms are foundational: without them, the UK cannot achieve the real-time resilience that modern fraud prevention demands.

---

4. Liability Drives Behaviour: Why the UK's Reimbursement Rule Matters

One of the most influential levers in fraud prevention is liability. When victims bear losses, institutions have limited incentive to invest in stronger protections. When institutions bear losses, the dynamic changes instantly.

The UK's October 2024 reimbursement rule is a prime example of this principle in action. By requiring all banks and PSPs to reimburse innocent victims of authorised push payment (APP) scams, the UK created an immediate and direct financial incentive for institutions to strengthen fraud defences. Reimbursement rates jumped from **56% to 88%** almost overnight. The industry now collectively absorbs approximately another **£150 million** annually in repayment costs.

This shift has driven banks to invest more aggressively in behavioural biometrics, advanced transaction monitoring, and high-speed detection tools. It has also increased collaboration across fraud teams, accelerated data sharing, and raised expectations for how institutions should respond to emerging fraud threats.
International comparisons are revealing. In the EU, liability still largely sits with the customer. Japan relies on a cultural framework—family consultation and public education—to reduce fraud, although regulators now require banks to refund 50% of investment scam losses. In the United States, liability varies, with mixed results and rising consumer losses.

Where liability sits, innovation follows. In the UK's case, shifting liability to institutions was the most important regulatory development in a decade.

This rule alone justifies the need for a 'Fraud Minister'. Incentive-driven policy requires central coordination, and the reimbursement rule created conditions under which fraud prevention became a strategic priority.

---

5. Restoring UK Leadership: A Decade of Lost Ground

The UK was once a global pioneer in payment modernisation. The Faster Payments Service, launched in 2008, transformed the speed of domestic money movement and inspired similar systems worldwide. Yet over the past decade, leadership has eroded.

The DPA project—one of the most successful fraud intelligence pilots ever run—was shelved despite clear evidence of impact. The highly anticipated New Payment Architecture (NPA), launched in 2018 to modernise the UK's payment infrastructure, was paused in 2024 after years of cost, uncertainty, and strategic drift. In 2025, the government introduced the New National Payment Plan, but clarity on delivery remains limited.

Industry frustration is clear. The Payment Association's "Payments Manifesto 2026" calls for structural reform, including a Police Reporting Trigger designed to streamline fraud investigations and ease liability pressures. The sector recognises that without a coherent national strategy, innovation cannot flourish and fraud cannot be contained.

Meanwhile, other regions have surged ahead. The EU has harmonised messaging standards, fraud regulations, and payment protocols. Asian markets have embraced digital identity frameworks and real-time verification systems. The US, despite its fragmented ecosystem, is investing in critical improvements through FedNow and enhanced fraud analytics.

The UK's legacy remains strong, but its competitive advantage has weakened. Reclaiming leadership requires coordination, investment, and the political mandate the new Fraud Minister now brings.

---

6. The Path Forward: Real-Time Intelligence, AI, and Cross-Industry Coordination

Modern fraud is agile, distributed, and increasingly powered by automation and AI. Criminals deploy scalable social engineering scripts, deepfake audio, spoofed caller IDs, cloned websites, and global mule networks that can move money across borders within seconds. To counter this, the UK must adopt a real-time, intelligence-led model of fraud prevention.

Banks and PSPs must integrate high-volume streaming analytics, risk scoring engines, and behavioural biometrics capable of assessing transactions in milliseconds. Machine learning models that analyse historical data must be paired with real-time signals—device fingerprints, geolocation anomalies, transaction velocities, and social media-linked scam indicators.

Yet technology alone is not enough. Fraudsters exploit silos. They rely on the fact that social media platforms do not coordinate with telecom providers, who do not coordinate closely enough with banks, who do not automatically share information with each other or with law enforcement. Criminal networks thrive in these seams.

The Fraud Minister's most critical responsibility is knitting these sectors together. The UK needs coordinated operational frameworks that integrate intelligence from social media, telecoms, banks, PSPs, law enforcement, and the public. Each sector holds a vital piece of the puzzle. None can address the threat alone.

If the UK can achieve real-time, cross-sector coordination, it will not only reduce fraud—it will set a new global standard for digital resilience.

---

7. Suggested Incentives: A New Framework for National Fraud Prevention

The long-term success of the UK's fraud strategy depends on incentives that drive cooperation, not just compliance. Industries respond to aligned economic signals. When incentives reflect national goals, coordinated behaviour follows.

Banks and PSPs once had little motivation to invest heavily in fraud prevention. Losses were often absorbed by victims, reputational risk was contained, and fraud teams operated discreetly. The new reimbursement rule changed that structure. By placing liability directly on institutions, the UK has transformed fraud from a reputational concern into a financial priority. Greater losses now mean stronger internal controls, more investment in AI systems, better customer education, and greater willingness to share intelligence.

Social media platforms remain the primary vector for scam initiation. With **75% of UK scams originating on these platforms**, they are the front line of the fraud ecosystem—yet they bear the least financial consequence. The EU's Digital Services Act, which allows fines of up to **10% of global turnover**, shows how meaningful penalties shift behaviour. Applying similar sanctions in the UK would incentivise platforms to invest in identity verification, scam detection algorithms, advertiser vetting, and rapid takedown systems. When inaction becomes expensive, action becomes strategic.

Law enforcement faces chronic delays in processing fraud cases, with current timelines ranging from two to three years. This makes digital fraud effectively low-risk for criminals operating at speed with disposable devices. Accelerated digital case handling, specialist fraud courts, expanded cyber-forensics units, and improved cross-border agreements would increase the certainty of detection—a far more powerful deterrent than harsher sentences alone.

Telecom providers play a critical role in combating impersonation scams, which often rely on number spoofing and fraudulent SMS messages. Enhanced incentives could require real-time caller ID authentication, cross-network scam intelligence sharing, and automated blocking of known fraudulent numbers. Pre-answer scam warnings should become standard.

For fraudsters, the greatest deterrent is not punishment but probability of detection. With faster investigative cycles, integrated intelligence platforms, and better international cooperation, the UK can raise detection rates and disrupt the criminal business model.

These incentive structures are not punitive; they are corrective. They re-align private sector behaviour with public interest and national security. If implemented consistently, they provide the missing architecture for a truly coordinated fraud prevention ecosystem.

Conclusion: A Pivotal Opportunity — If the UK Moves with Urgency

The appointment of the UK's first Fraud Minister is a watershed moment. For the first time, the UK is treating fraud as a strategic threat requiring national coordination. Lord Hanson's early outline—a three-year plan supported by initial funding, a 400-strong National Fraud Squad, and more robust regulatory tools—signals seriousness. But the challenge ahead is formidable.

Entrenched institutional cultures, fragmented data systems, and legacy payment infrastructure continue to limit progress. Cross-border cooperation remains inconsistent. Funding will need to increase to meet the scale of the threat. And execution must be swift, decisive, and relentless.

Yet the opportunity is real. The UK can reclaim global leadership in fraud prevention by aligning incentives, investing in real-time intelligence, enforcing cross-sector collaboration, and leveraging modern regulatory frameworks. In doing so, it can strengthen the financial system, protect citizens, and reinforce the international stature of The City.

Three years is not long. But with strong leadership, aligned incentives, and real-time coordination, it is enough to transform the nation's fraud capability. The mandate is clear. The urgency is real. And the window for leadership is open.