Banking
Risk & Regulation

Analysis, Compliance

Patchy data reconciliation weakens banks' compliance shield

By Victor Smart

June 16, 2025

Banks' efforts to meet regulatory demands on fraud and cyber attacks are threatened by the payments systems' "messy" data, say experts.

A ranking of 31 leading processing firms by fintech Kani raises questions around data quality.

According to an in-depth analysis by the reconciliation and reporting platform, only one in four (eight) payment processing firms, which handle transactions on behalf of banks and card networks, have fit-for-purpose data.

Meanwhile, the same number fails to meet their core requirements regarding reconciliation, reporting, regulatory compliance and financial oversight.

The deep dive by Kani does not disclose who has 'failed', but lists Clowd9, DPG, Enfuce, Paymentology, and Thredd as among the top performers.

Speaking from an industry-wide perspective, Lee Travers, CEO of fintech transformation consultancy Fintech Futures, says: "Patchy systems invite cyberattacks and are a fraudster's playground.

"In incumbent banks, risk and compliance teams are tearing their hair out over dodgy data [sent from merchants to card networks via payment processors] and operational risk."

Jamie Allsop, of tech solutions firm HTEC, says 'reconciliation' — where transactions match up with a bank's records — is a "mess". "Meanwhile, regulators are raising expectations faster than many institutions can keep up," he adds.

Cloud on the horizon

Nine of those processors assessed have minor deficiencies, affecting efficiency, the report adds. A further six require "prompt remediation". The survey says the most common failure among data processors is the inability to perform daily reconciliation.

That can be due to missing fees, settlement fields or bank identification numbers, even though these are part of the basic regulatory requirements.

Aaron Holmes

"Even large, established businesses often don't realise their data is incomplete until a failure occurs," says Kani CEO Aaron Holmes.

He says it is not always the clunky legacy systems that perform worst. In fact, they still can handle data accurately and promptly.

Instead, some modern transaction-processing platforms built on cloud and API-based software can be flawed.

Holmes says they provide "a veneer" of sophistication on data communications, while the underlying payments system still relies on a mix of old and new architectures built up over decades.

"In some banks, mainframe systems from the 1960s and 1970s are still in use, so old that many specialist software engineers have retired," says Holmes.

These legacy systems connect to real-time payment networks like the Mastercard and Visa card rails.

These must be integrated with banks' new user-friendly API interfaces and enable mobile banking, digital wallets and other new financial products.

"A transaction might be authorised in milliseconds, yet reconciliation can take hours or even days," says Holmes.

Fadl Mantash, chief information security officer at UK paytech Tribe Payments, says: "Fraud detection relies on pattern recognition, and you can't spot patterns if half the data is missing or malformed."

He adds that when new regulations come along, such as the ISO 20022 SWIFT messaging standard due this November, the system struggles to adapt.

Fraud breakdown

A sharp spike in fraud and cyberattacks has prompted regulators to ramp up the pressure.

Nicole Sandler, from the Centre for Finance, Innovation and Technology, a UK government-backed taskforce, adds: "Many systems still operate in silos.

"This lack of interoperability creates significant operational drag for compliance teams, which means that illicit activity can go undetected or, if it is identified, it can be too late.

"If you don't have proper data sharing, this opens up new vectors for fraud. Scammers exploit lags and mismatches in onboarding, and red flags that could be raised are not raised."

Loss on a 'technicality'

Beyond fraud and cybersecurity, one of regulators' most urgent concerns is safeguarding individuals' funds held by electronic money institutions, firms which can process transactions and bank accounts.

EMI status, which does not permit customer lending, is the first step many challenger banks take to become full banks.

Supervisors require that clients' money is ring-fenced and not mixed with working capital.

But a High Court case unsuccessfully brought by the Financial Conduct Authority in 2021 over the collapse of an EMI called Ipagoo exposed weaknesses in the system. "A lot of firms think they are safeguarding properly but simply aren't meeting the standards," says Holmes.

Experts believe financial institutions are now confronting the reality of their "technical debt": the costs banks face due to failure to future-proof integration with legacy data systems

"Some banks have chosen to put a Band-Aid over a gaping hole rather than redoing the infrastructure thoroughly," explains Sandler.

In with the old

Mariajo Bastero, commercial director at AI anti-fraud experts Lynx, believes newer tech can adjust to the rapidly changing scamming landscape. "Newer fraud prevention solutions focus on adaptability and real-time learning," she says.

"These systems can adjust to emerging fraud patterns and maintain high detection accuracy. The way forward for financial institutions involves integrating these adaptive technologies into their fraud prevention strategies, ensuring they remain resilient."

But scrapping the legacy systems outright seems a non-starter.

Radi el Haj, CEO of payments technology firm RS2, warns: "Companies should not go all-in on removing their legacy technology immediately.

"We have seen that it is far safer and more efficient to gradually transition to modern technology."

Holmes comments: "We are still stuck for the moment with many of the systems from the 1960s and 1970s, but regulators will not, in the current climate, tolerate a failure to tackle issues like fraud."

Kani undertook a long-term analysis of 31 leading processing firms over the last 24 months. It highlights issues with poor data completeness, accuracy and consistency. Feedback has been passed on to individual data providers to help improve the quality of their data files.