Financial crime in fintech times

Fraud is growing fast and it's costly.

So, here's the dilemma: One of the goals of fintech is to facilitate faster, freer movement of finances that enhance the user experience. But with fraud and financial crime evolving as rapidly as the services they target, how do you protect legitimate consumers while not introducing the kind of measures that make their experience slower, more cumbersome and, ultimately, not worth the effort?

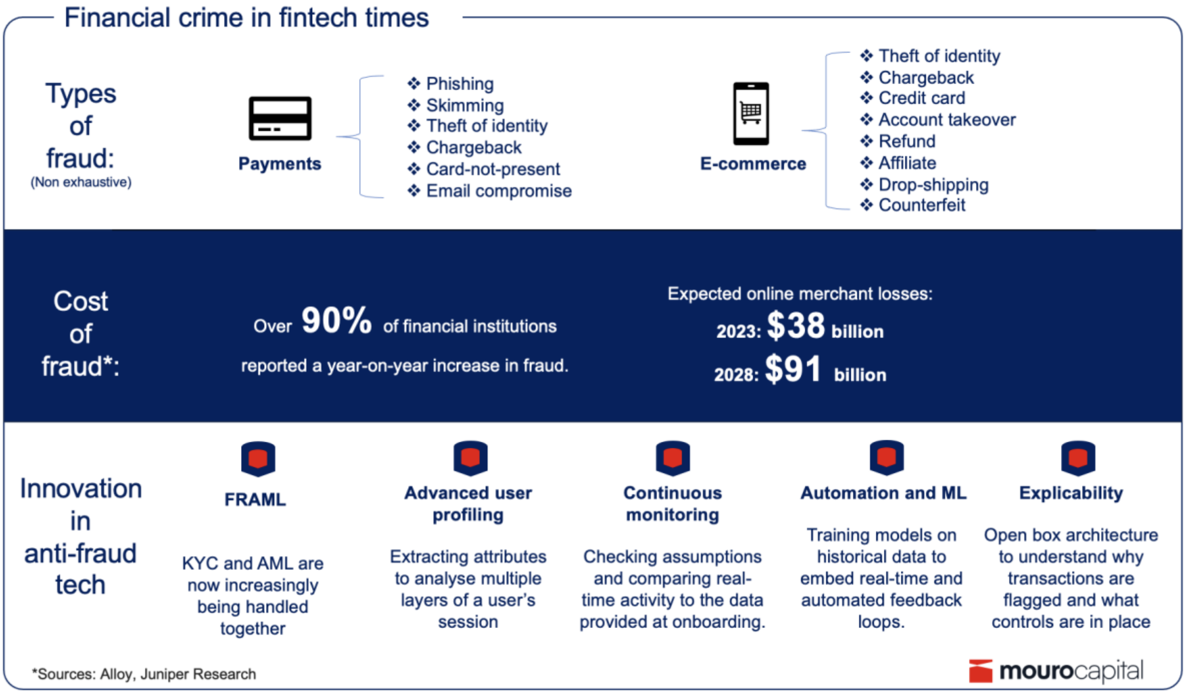
Fraud touches many verticals in addition to financial services. It has a broad definition including transactional fraud and mobile app fraud, biometric id fraud, and synthetic id fraud, among others. While technology has made strides in preventing fraudulent activity, fraudsters have concurrently evolved, becoming more sophisticated and challenging to detect. Phishing scams have grown in magnitude and complexity, and we are currently experiencing how emerging technologies like generative AI and ChatGPT are blurring the lines between genuine and fraudulent information, adding complexity to the task of combating fraud.

As a consequence, according to Alloy, last year 91% of financial institutions reported a year-on-year increase in fraud, and 71% increased their spending to combat it. Whether it's increased cost to prevent fraud or fines for non-compliance, overall costs for financial institutions translate in hundreds of billions of dollars annually.

Fraud-related costs are high across industries. E-commerce activity has surged in recent years and is projected to reach $8.1 trillion worldwide sales by the end of 2026. Digital payments growth is strongly correlated with payments fraud, with some forecasts predicting losses to fraudulent activity to reach more than $340 billion between 2023 and 2027.

Moreover, merchants face higher costs in terms of lost sales due to strict verification requirements like two factor authentication and/or poor customer verification and onboarding. Online platforms are forced to block a large percentage of purchases to keep fraud at reasonable levels — as large as 10-15%, depending on the vertical.

Fraud occurs at each step of the customer journey, from account opening to transaction and delivery. So, for companies, and risk and compliance solution providers the key question is **'how to improve the customer journey and sales conversion rate while blocking fraud and identity theft?'**.



Financial crime in fintech times

Types of fraud: (Non exhaustive)

Payments
- Phishing
- Skimming
- Theft of identity
- Chargeback
- Card-not-present
- Email compromise

E-commerce
- Theft of identity
- Chargeback
- Credit card
- Account takeover
- Refund
- Affiliate
- Drop-shipping
- Counterfeit

Cost of fraud*:

Over **90%** of financial institutions reported a year-on-year increase in fraud.

Expected online merchant losses:
2023: **$38** billion
2028: **$91** billion

Innovation in anti-fraud tech

FRAML
KYC and AML are now increasingly being handled together

Advanced user profiling
Extracting attributes to analyse multiple layers of a user's session

Continuous monitoring
Checking assumptions and comparing real-time activity to the data provided at onboarding.

Automation and ML
Training models on historical data to embed real-time and automated feedback loops.

Explicability
Open box architecture to understand why transactions are flagged and what controls are in place

*Sources: Alloy, Juniper Research

mourocapital

New PSD2 regulations seek to help reduce the spread of fraud in Europe by requiring payment providers to implement two factor authentication for transactions. In doing so, they shift responsibility for fraud prevention from the merchant to the payment provider themselves. But this has led to a large reduction in transaction conversion rates, with a growing number of shoppers abandoning their purchase at the authentication stage or failing to pass the two-factor hurdle. According to Forter, the average 3-D Secure - a protocol designed to be an additional security layer for online credit and debit card transactions - success rate can be as little as 60%, with 17-20% of transactions abandoned and the remainder failing.

But here's the call to action for fintechs: numerous opportunities exist for players, especially in the regtech space, to innovate solutions. Both legacy financial institutions and fintechs themselves are in dire need of an approach that can optimise processes for fraud prevention, reducing losses to bad actors and enshrining commercial productivity through a positive customer experience.

The first wave of innovation came from developing strong rules-based platforms that analyse web traffic or transactional data to detect fraud, based on historical patterns and statistical models. To give an example, VISA acquired CyberSource in 2010 to do just that, and more recently, Kount has joined Equifax. Innovation has evolved by leveraging additional data and developing machine learning and deep customer profiling. As an example, Ravelin combines machine learnings, graph networks, behavioural analysis to detect fraud and increase payment acceptance. Nethone helps e-commerce and financial institutions reduce payment fraud through advanced end-user session profiling focusing on mobile channels. Seon focuses on identifier reputation checks which include enriching context on a purchaser based on identifiers (email, phone number and IP address) passed via APIs.

While fraud, KYC and anti-money laundering (AML) efforts were previously kept in separate silos, they are now increasingly being handled together in what is known as a "FRAML" approach, like Hawk AI's. This holistic approach blends fraud and AML in other operational areas, which can be in the context of onboarding and personalisation to improve conversion rates, or as part of risk assessment for underwriting decisions in other cases for fraud and KYC.

But diving into a bit more detail: what are the successful characteristics that will enable players in this space to enhance customer journeys and conversion rates while mitigating the risks of fraud and identity theft?

Data accuracy

Traditionally, the focus has been on accuracy. This means a strong performance related to identifying false positive/negative, and which further underlines the importance of looking at data holistically to identify patterns more easily. Advanced end-user profiling extracts user attributes to analyse several layers of a user session and identify, for example, whether it is a human or a bot completing the transaction.

Continuous Monitoring

Fraud protection doesn't begin and end with the individual controls in place but relies on continuous monitoring to check assumptions and compare real-time activity to the data provided at onboarding. Friction and accuracy are seen as trade-offs in this instance. On-boarding and data storage in one solution can help rise to the challenge; having local data centres can be costly but speeds up processing for real-time monitoring and helps clear regulatory hurdles related to local data management.

Automation

Machine learning models enable a real-time and automated feedback loop. This involves training models on historical data to learn patterns of behaviour and detect anomalies or suspicious activity; it can also help speed up suspicious activity reporting by taking out the manual component. Machine learning algorithms can adapt to new fraud patterns by continuously retraining the models.

Explicability

Open box architecture helps merchants and financial institutions understand why a transaction is flagged and provides extra flexibility in determining what controls to put in place. Crucially, this helps customers who have, or want to develop their own in-house fraud models or use data for complementary purposes.

On top of the above technological considerations, it is important to consider for product, commercial and regulatory aspects.

Expanding to new use-cases

The capability to maintain high approval rates with low fraud incidence when expanding to new use cases is important, not only from a product perspective but also in the context of the business model. By taking on risk, a provider opens itself to negative impact on cost structure, particularly with a number of anti-fraud providers offering chargeback guarantees as part of their service. If the provider doesn’t stay ahead of the game, they can suffer gross margin losses due to higher chargebacks. This is also the case when serving new products; digital goods like crypto are particularly at risk because goods are transferred instantly, allowing less time to spot the fraud than in the case of e-commerce, where products are shipped within a few days.

Partner prioritisation

Careful choices about who best to partner with — underlying merchants or the payment provider — can be make or break. Underlying merchants have more data, but the payment provider confers scale and some degree of indemnity.

What’s more, partnering with payment providers can help merchants reduce 3DS conversion losses. The introduction of Strong Customer Authentication (SCA) in the UK and Europe has created an extra incentive to keep fraud rates low, and doing so will allow more exemptions from two-factor authentication and SCA requirements. Payment Service Providers (PSPs) with fraud rates below 0.13% can exempt transactions of less than €100; under 0.06% allows for exemptions below €250, and under 0.01% allows for exemptions below €500. Merchants ought to like this, as it creates higher acceptance rates and smoothes the way at checkout.

Channel prioritisation

Cross-channel and multi-channel capabilities like web and mobile are becoming increasingly important, especially in emerging markets which have a mobile first approach. A risk approach that treats the two symbiotically, comparing data and monitoring across platforms, can only enrich efforts to counter fraud.

In all likelihood, this is an unending cycle of activity — vicious or virtuous, depending on your point of view. Companies will always seek to make it easier for their customers to transact with them and bad actors will always find a way to exploit the system for their own benefit. But, for as long as the ecosystem exists, there is good business for smart fintechs in both boosting the customer journey and making it safer to do so.