feedzai

A Collection of Resources for Banks:

PSD2 & Strong Customer Authentication

Transforming PSD2 and Strong Customer Authentication into Opportunities

PSD2: How Machine Learning Reduces Friction & Satisfies SCA

PSD2 Payments Authentication Workflow: A Blueprint

Introduction

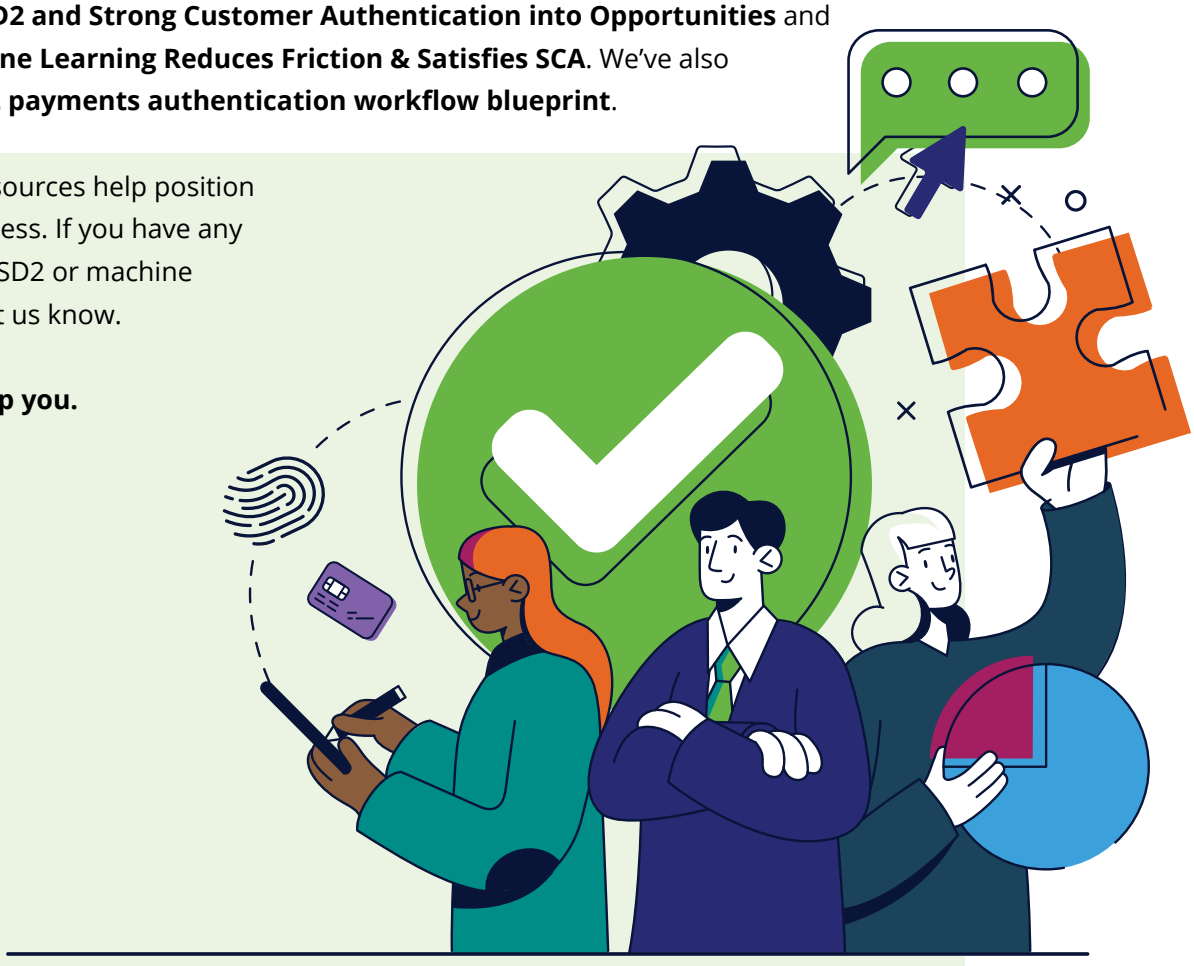
The Second Payment Services Directive (PSD2) seeks to increase competition and innovation for the benefit of consumers. As with most large initiatives, it's not without irony. Open Banking requires banks to share their customer's data in a standardized format with third-party payers, while simultaneously protecting customers, and themselves, from fraud.

Preparing for PSD2 is no small feat, as indicated by the fact that the European Union pushed back the deadline a few times already. As of this writing, SCA compliance is required by December 31, 2020. Will that change? It's possible. The Coronavirus pandemic could further delay the deadline. But we do know that sooner or later, full compliance will be required. And banks must prepare today for tomorrow's inevitability.

Feedzai helped a major U.K. bank become the first bank to fully comply with PSD2. In PSD2 & Strong Customer Authentication: A Collection of Resourcesfor Banks, we share our pivotal articles **Transforming PSD2 and Strong Customer Authentication into Opportunities** and **PSD2: How Machine Learning Reduces Friction & Satisfies SCA**. We've also included our **PSD2 payments authentication workflow blueprint**.

We hope these resources help position your bank for success. If you have any questions about PSD2 or machine learning, please let us know.

We're here to help you.



Transforming PSD2 and Strong Customer Authentication into Opportunities

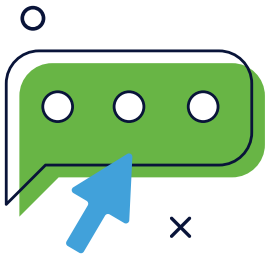
By: Saurabh Bajaj

Although some delays were recently announced for Strong Customer Authentication (SCA), an important part of PSD2, the pressure for all payment service providers (PSPs) to make sure their systems are compliant and customer-centric continues to mount. As fraud increases, customer behaviours change, and a more competitive open banking market becomes the reality, PSPs have to work continuously to manage risk and reduce friction. This includes increasing security measures around customer authentication to prevent customer attrition in this hyper-competitive era.

However, there are critical steps PSPs can take to make their goals easier to achieve. This includes examining the exemptions found in Article 18 of the Regulatory Technical Standards, which support PSD2 and set out Strong Customer Authentication (SCA) requirements. By drawing on this knowledge, PSPs can leverage certain capabilities to easily stay compliant while improving the client user experience. This paper explores these steps, revealing how a robust machine learning (ML) solution is key for PSPs that want to turn regulations into opportunities.

SCA: exemptions and implications

One of the main PSD2-related areas of focus is SCA, which aims to increase trust through authentication and improve security. It requires PSPs to provide two out of the three following items to verify identity:



Something you know
(password, response to a security question, PIN);

Something you have
(two-factor authentication via mobile phone, hardware token, smart card);

Something you are
(Fingerprint or facial recognition);

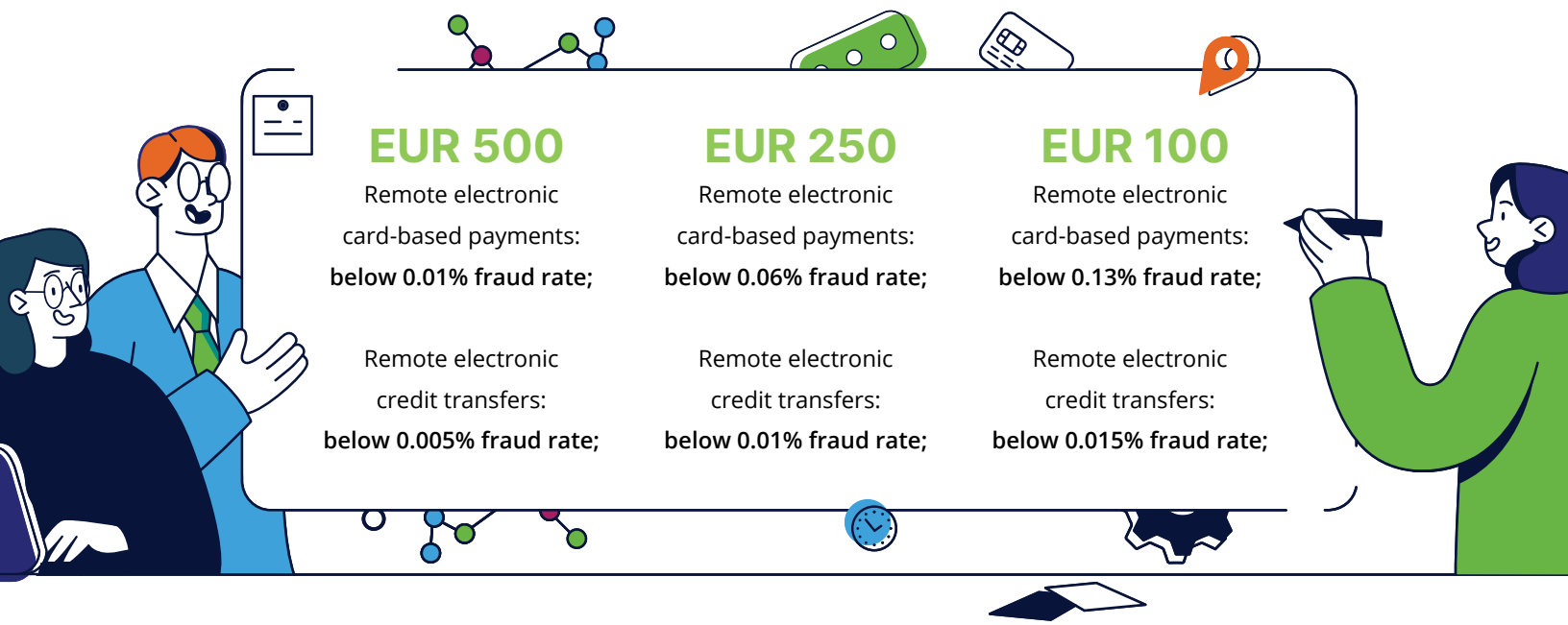
SCA isn't applied to some transactions that are considered low risk, including balance checks, low-value transactions (<EUR 30 for a single transaction), and the number or amount of transactions relative to the last time SCA was performed. However, since one of SCA's aims is to increase security for transactions that can't immediately be deemed as low-risk, these exemptions do not cover all low-risk transactions. For instance, if you have a nice dinner with a friend and later reimburse them EUR 100 for dinner, you might undergo SCA even though the transaction seems low-risk to you.

Due to the exceptions and the fact that not all of them cover genuine low-risk transactions, customers can easily become confused and irritated as to why they're encountering friction. For instance, they may be baffled about why some low-risk transactions are subjected to SCA and others are not, or why they themselves are put through SCA when they haven't committed fraud. As valuable customers are exposed to more friction through unnecessary SCA, they may flee to competitors that can validate these transactions without SCA intervention.

In addition to the exemptions to SCA, there are also exceptions to these exemptions. This is where machine learning can be used – when it comes to remote transactions that fall above EUR 30 and up to EUR 500.

Machine learning: a customer-centric and competitive advantage

This is an exception because fraud prevention platforms that use machine learning to identify and prevent fraudulent activity directly help decrease fraud rates of the banks they service. These platforms use advanced ML to avoid unnecessary SCA for users because they drive fraud rates down to a level that is deemed allowable for exemption. See below the reference fraud rates for certain transaction values:



Robust machine learning makes these rates easy to achieve. Platforms with these capabilities provide a customer-centric and competitive advantage to the PSPs that use them.

PSPs that don't use machine learning to drive down fraud rates are at a significant disadvantage: this exemption to SCA (i.e. exemption about remote transactions between the EUR 30 - EUR 500 threshold) wouldn't apply to them. More specifically, banks that don't take advantage of the SCA exemptions for transactions in the defined threshold are essentially asking their customers to undergo unnecessary friction, simply because they are unable to accurately identify transactions as low-risk or high-risk.

In an open banking landscape, where more and more competition is being introduced, it's critical for banks to reduce customer friction to avoid driving customers and applicants away. To do so, banks must eliminate SCA when they can.

A platform and partner for improved security

PSD2 aims to increase competition in the banking landscape, which benefits consumers and helps even out the playing field for established and emerging PSPs. However, opening up the banking landscape to more competition opens it up to more fraud.

As a result of PSD2, any institution that holds customer data and account information needs to provide new PSPs access to that data and account information via an API. This allows customers to choose how they view their data, either through their traditional banking accounts or through new third parties that consolidate all of their account information in a single platform. Although this is great for the customer, it means that PSPs now need to watch out for fraudsters and make sure they're sharing sensitive data information with other parties securely.

This is where having an ML fraud prevention platform is imperative to data security, as data is shared more openly amongst various players. This way, PSPs can prevent and quickly detect fraud without raising their operational teams' costs or interfering with customers' experiences.

Furthermore, since fraudsters can attack multiple payment methods, PSPs may find it helpful to partner with a machine learning company that works on the full life cycle of the payment industry, which could easily guide the clients in AI techniques that are used by other players in the life cycle (e.g. merchants, processors, and acquirers).

PSPs must consider a tremendous number of factors when it comes to complying with regulations while trying to outmanoeuvre their competition. However, those that use machine learning for fraud prevention can breathe a sigh of relief, knowing they have the technology in place to decrease fraud rates and help them succeed in the world of PSD2.

Pedro Barata,
Senior VP of Product, Feedzai
Where he leads product development and management to bring the most advanced financial crime fighting technology to market. Prior to joining Feedzai, Pedro worked for Critical Software, where he helped design and develop systems for CMMi appraisals, globally supporting project management initiatives.

PSD2: How Machine Learning Reduces Friction & Satisfies SCA

By: Andy Renshaw

It crosses borders but doesn't have a passport. It's meant to protect people but can make them angry. It's competitive by nature but doesn't want you to fail. What is it?

If the PSD2 regulations and **Strong Customer Authentication (SCA)** feel like a riddle to you, you're not alone. SCA places strict two-factor authentication requirements upon financial institutions (FIs) at a time when FIs are facing stiff competition for customers. On top of that, the variety of payment types, along with the sheer number of transactions, continue to increase.

According to **UK Finance**, the number of debit card transactions surpassed cash transactions as long ago as 2017, while mobile banking surged over the past year, particularly for contactless payments. Whatsmore, the number of contactless payment transactions per customer is growing. This increase in transactions also raises the potential for customer friction.

The number of transactions isn't the only thing that's shown an exponential increase; the speed at which FIs must process them is too. Customers expect to send, receive, and access money with the swipe of a screen. Driven by customer expectations, instant payments are gaining traction across the globe with **no sign of slowing down**.

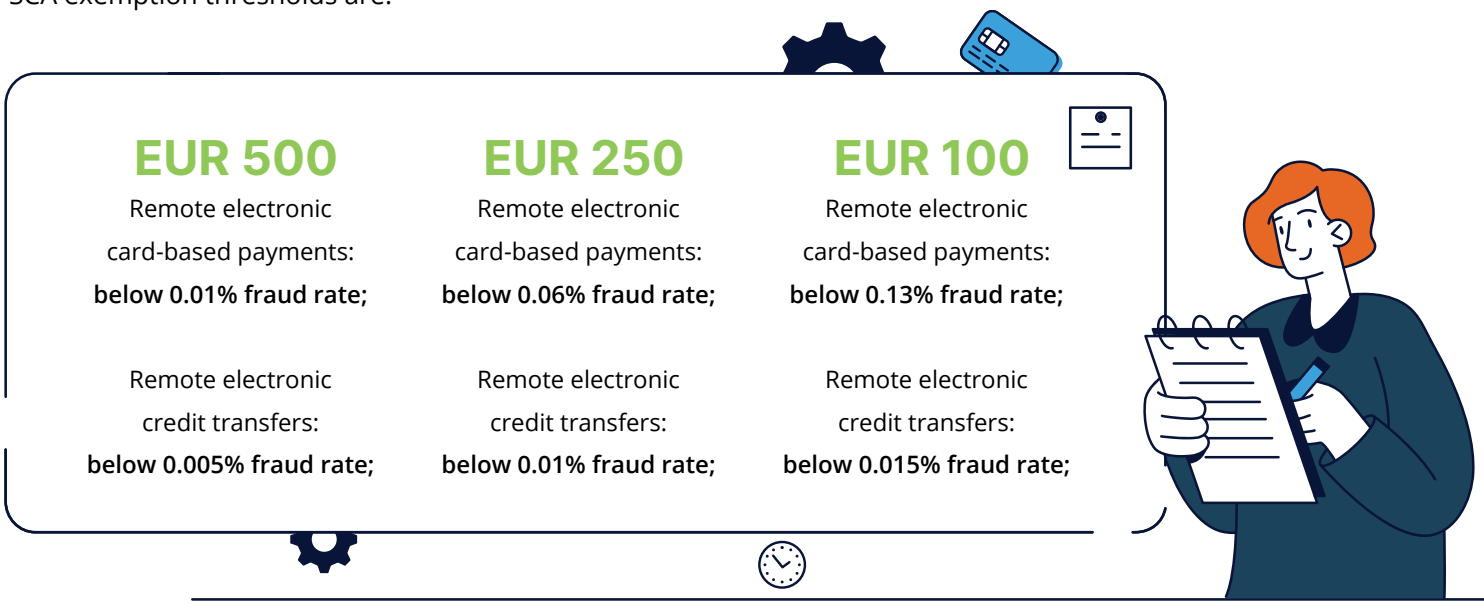
Considering the sheer number of transactions combined with the need to authenticate payments in real-time, the demands placed on FIs can create a real dilemma. In this competitive environment, how can organizations reduce fraud and satisfy regulations without increasing customer friction?

For countries that fall under PSD2's regulation, the answer lies in the one known way to avoid customer friction while meeting the regulatory requirement: keep fraud rates at or below SCA exemption thresholds.

How machine learning keeps fraud rates below the exemption threshold to bypass SCA requirements

Demonstrating significantly low fraud rates allows financial institutions to bypass the SCA requirement. The logic behind this is simple. If the FI's systems can prevent fraud at such high rates, they've demonstrated their systems secure without authentication.

SCA exemption thresholds are:



Looking at these numbers, you might think achieving SCA exemption thresholds is impossible. After all, bank transfer scams **rose 40%** in the first six months of 2019. But state-of-the-art technology rises to the challenge of increased fraud. Artificial intelligence, and more specifically machine learning, makes achieving SCA exemption thresholds possible.

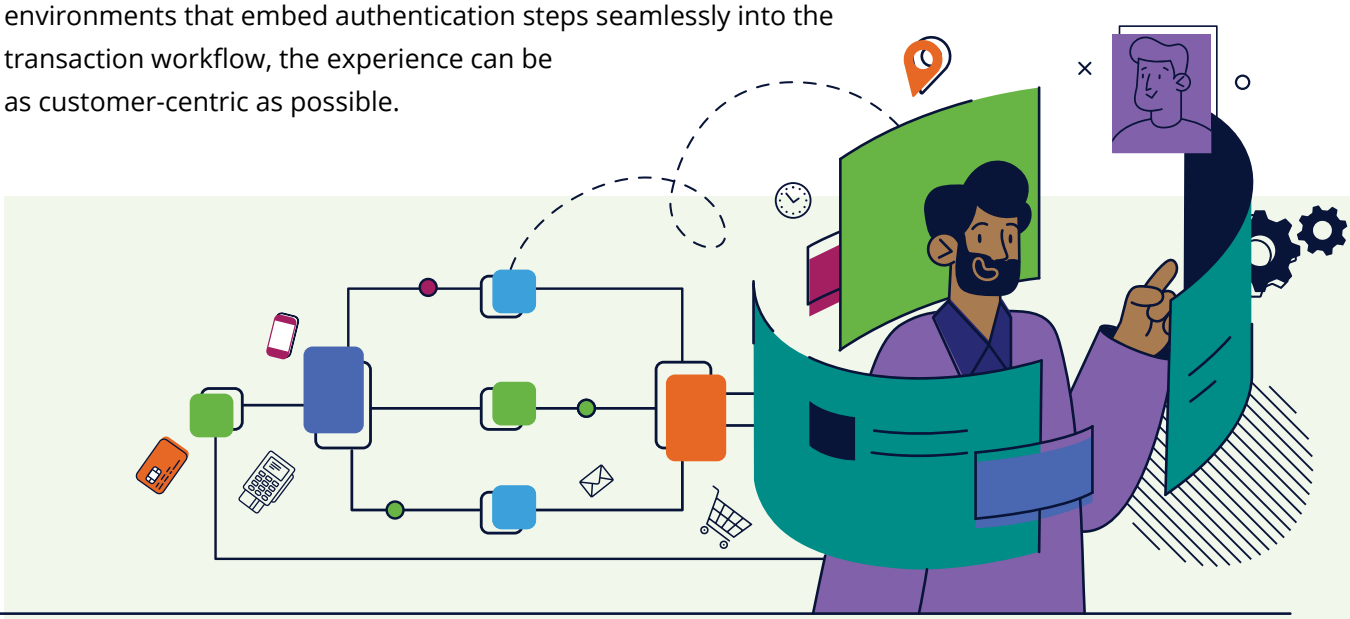
How machine learning achieves SCA exemption threshold values

Every transaction has hundreds of data points, called entities. Entities include time, date, location, device, card, cardless, sender, receiver, merchant, customer age — the possibilities are almost endless. When data is cleaned and connected, meaning it doesn't live in siloed systems, the power of machine learning to provide actionable insights on that data is historically unprecedented.

Robust machine learning technology uses both rules and models and learns from both historical and real-time profiles of virtually every data point or entity in a transaction. The more data we feed the machine, the better it gets at learning fraud patterns. Over time, the machine learns to accurately score transactions in less than a second without the need for customer authentication.

Machine learning creates streamlined and flexible workflows

Of course, sometimes, authentication is inevitable. For example, if a customer who generally initiates a transaction in Brighton, suddenly initiates a transaction from Mumbai without a travel note on the account, authentication should be required. But if machine learning platforms have flexible data science environments that embed authentication steps seamlessly into the transaction workflow, the experience can be as customer-centric as possible.



Streamlined workflows must extend to the fraud analysts job

Flexible workflows aren't just important to instant payments, they're important to all payments. And they can't just be a back-end experience in the data science environment. Fraud analysts need flexibility in their workflows too. They're under pressure to make decisions quickly and accurately, which means they need a full view of the customer — not just the transaction.

Information provided at a transactional level doesn't allow analysts to connect all the dots. In this scenario, analysts are left opening up several case managers in an attempt to piece together a complete and accurate fraud picture. It's time-consuming and ultimately costly, not to mention the wear and tear on employee satisfaction. But some machine learning risk platforms can show both authentication and fraud decisions at the customer level, ensuring analysts have a 360-degree view of the customer.

Machine learning prevents instant payments from becoming instant losses

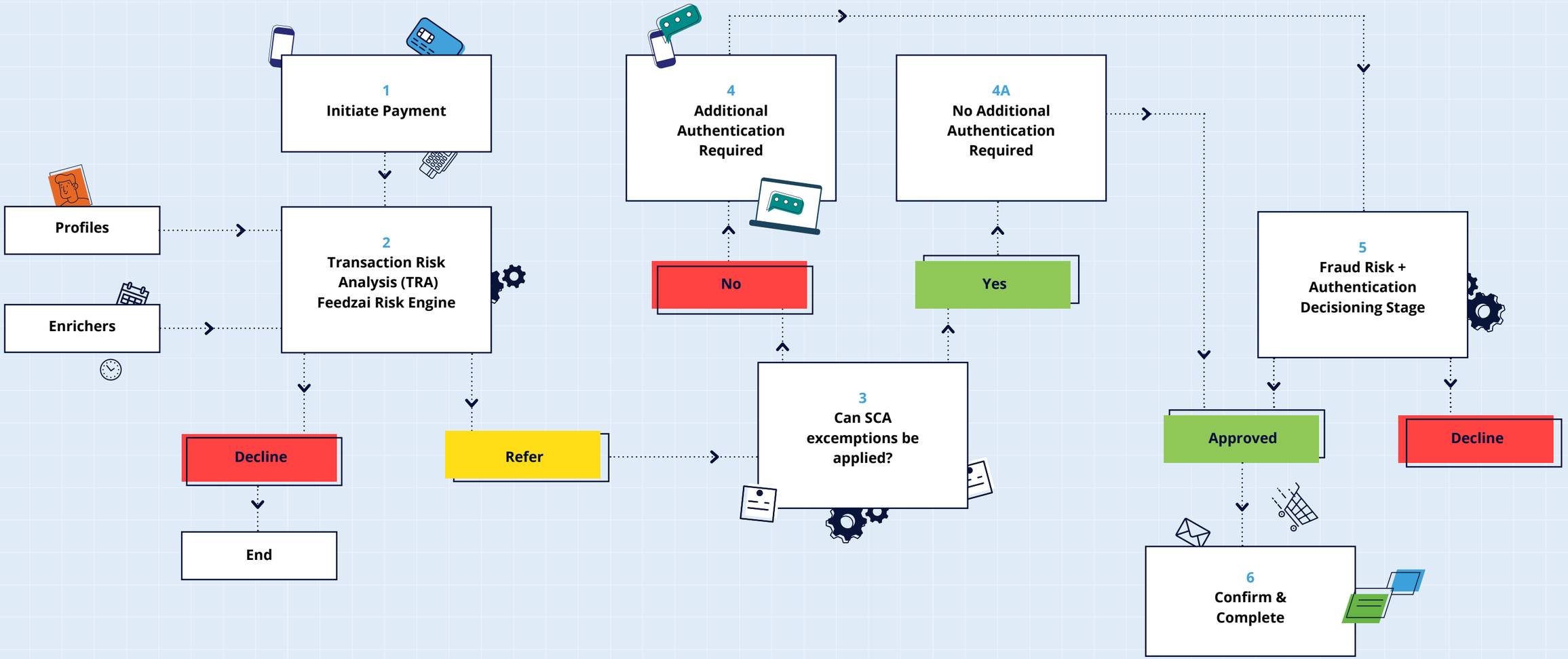
Instant payments can provide immediate customer satisfaction, but also instant fraud losses. Scoring transactions in real-time means institutions can increase the security around the payments going through their system before it's too late.

Real-time transaction scoring requires a colossal amount of processing power because it can't use batch processing, an efficient method when dealing with high volumes of data. That's because the lag time between when a customer transacts and when a batch is processed makes this method incongruent with instant payments. Therefore, scoring transactions in real-time requires supercomputers with super processing powers. The costs associated with this make hosting systems on the cloud more practical than hosting at the FIs premises, often referred to as "on prem.". Of course, FIs need to consider other factors, including cybersecurity concerns before determining where they should host their machine learning platform.

Providing exceptional customer experiences by keeping fraud at or below PSD2's SCA threshold can seem like a magic trick, but it's not. It's the combined intelligence of humans and machines to provide the most effective method we have today to curb and prevent fraud losses. It's how we solve the friction-security puzzle and deliver customer satisfaction while satisfying SCA.

Andy Renshaw,
VP, Banking Solutions
15 years of experience in banking and the financial services industry, leading large programmes and teams in fraud management and AML. Prior to joining Feedzai, Andy held roles in global financial institutions such as Lloyds Banking Group, Citibank, and Capital One, where he helped fight against the ever-evolving financial crime landscape as a technical expert, fraud prevention expert, and a lead product owner for fraud transformation.

PSD2 Payments Authentication Workflow: A Blueprint



feedzai

One Platform to Manage Financial Crime

Build Your Business. We'll Protect it.

Every day, Feedzai's enterprise risk management platform scores trillions of dollars of transactions to protect the world's largest companies. Architected to be fully AI-enabled to stay ahead of emerging financial crime and money laundering patterns, Feedzai mitigates even the most deceptive criminals so that merchants, issuers, and acquirers can focus on growth.

feedzai.com/feedzai-platform/

feedzai.com info@feedzai.com sales@feedzai.com