ThreatMetrix®
The Digital Identity Company™

5 Keys to Successful PSD2 Implementation

By Alisdair Faulkner

Publishing a new set of standards is one thing, but implementing them is another thing all together.

Now that banks and others in the financial services industry have had time to absorb the final Regulatory Technical Specifications (RTS) on Strong Customer Authentication (SCA) under PSD2, some may be wondering — what do we do now?

To be sure, PSD2 is set to accelerate the pace of disruption. Among other things, it mandates that banks open their payment account data to third parties through APIs, and to securely authenticate the account access and payment authorizations made through them.

This has understandably caused more than a little heartburn throughout the industry. So much so, in fact, that U.S. banks are actively lobbying to prevent such regulations from migrating stateside.

But it's also true that PSD2 promises to turbocharge innovation — not just for third parties, but for banks. Indeed, banks actually find themselves in pole position for capitalizing on some of the key advantages they will keep (and even gain) under PSD2.

PSD2 "doesn't threaten the existence of banks," according to Maikki Frisk, executive director for Payments Journal. "Instead, it presents a whole range of new opportunities for those that can adjust to the new environment: Better relationships with customers. New services. New revenues. Competitive advantage" and more.

But they'd better hurry. The RTS has been submitted to the European Parliament for ratification, and member states must roll its provisions into their national legal frameworks sometime in the next nine months. By November 2018, PSD2 is set to become law throughout the EU.

Make no mistake: For banks, whatever their own innovation agendas may be, success in the era of open banking is predicated most on their role as providers of secure authentication—as mandated by the RTS.

Getting Started: Five Keys to Successful Implementation

For the last several years, we've been working with some of the world's leading financial institutions to deliver real-time fraud detection and prevention for both risk-based authentication (RBA) and, increasingly SCA, using next-generation digital identity solutions.

Based on this experience, we've identified the five most important keys for a successful PSD2 implementation.

Think Beyond PSD2

Deploying solutions to meet the structures of the RTS is a baseline requirement, but systems must also be flexible enough to accommodate change as the market evolves.

PSD2 will have such a transformative impact on so many facets of the industry that there are bound to be modifications along the way. That includes the need to modulate against new innovations from

cybercriminals seeking to maintain and build upon the revenue streams they presently generate now that one in every three fraud attacks is successful.

To put it another way, PSD2 may have been proposed a decade after the original payment services directive. But with the dramatic pace of technological change, it might be sooner than you think before we're talking about PSD3.

Go Multi-Modal

The RTS calls for SCA for purchases above €30, and a cumulative limit of €100 on five consecutive payments. There are also exceptions up to €500 if the merchant's payment service provider meets stringent fraud rates. For everything else, RBA is allowed for faster payment.

However, this kind of friction caused by SCA can result in a 4-percent loss in sales and overall transaction volumes—cutting into revenues for both banks and merchants.

Financial institutions will want to deploy digital identity systems for seamlessly handling SCA- and RBA-based authentication. These solutions leverage dynamic digital identity intelligence, advanced behavioral analytics, adaptive policy engines and more to stop fraud at lightning-fast speeds without user friction.

Mobilize Cross-Purposefully

In perhaps its most significant directive, the RTS requires that mobile devices may be used as "multipurpose" devices for SCA and other applications, even if the payment service provider (PSP) only controls its own app or software on the device.

In fact, multifactor authentication can be achieved on the same device so long as it operates separately and securely from the environment hosting the PSP's application. Mechanisms must also be in place to ensure that neither the device or app has been altered — and to mitigate the impact if one or both has.

To facilitate this level of functionality for SCA, ThreatMetrix has extended its core technology platform to enable the customer's mobile device to become the authenticator and the enabler. This will include a crypto-based PKI certificate to ensure the device in question is the same device that was originally registered. It will also include push notification similar to two-way SMS challenge flows used for security notifications on iOS and Android platforms. There will also be cryptographically-backed biometric step-ups depending on use case.

Remember: Context is Everything

The European Banking Authority (EBA) states that users' previous spending patterns, transaction history, and location at the time of transaction must be used to identify anomalies in payment requests that may signal fraud.

These are just a few of the attributes used by ThreatMetrix to evaluate the true digital identity of end customers in real time. Others include device ID, IP address, geo-velocity, user credential attributes, mobile device integrity and more.

Our unique approach includes leveraging anonymized, crowd-sourced personal information that establishes the ever-changing associations between users and their devices, locations, behavior and more. Not by simply using a bank's own internal and partner data. Rather, globally—across tens of thousands of websites and millions of daily transactions in multiple industry categories.

By operationalizing the Digital Identity Network, banks can strike a balance between security and convenience across all customer touch points and payment mechanisms, as well as new API and consumer consent flows.

Make Security the Mother of Invention

The same mechanisms banks must put into place to comply with open banking standards can also be used to optimize the APIs they develop to support innovation from internal and partner initiatives.

Using digital identity solutions, financial institutions can prioritize the customer experience and maximize the lifetime value of new and existing customers, all while leveraging global, crowdsourced intelligence to keep them secure.

So Much to Do, So Little Time to Do It

Sure, there's always a chance the European Parliament will make modifications before approving the final RTS. But any such changes are likely to be minimal, and the directive is still set to become law in 17 months.

With apologies to an old proverb, that means the best time to get started was last month. The next best time is now.

For more information, read the exclusive white paper on how to implement a minimally invasive, strong authentication solution using turnkey solutions from ThreatMetrix.