truvity

Payments & Identity: Pains, Regulations, and How to Solve Them

A Truvity White Paper / 2024

Index

Introduction

The payments industry is rapidly evolving, presenting businesses with a range of challenges that need to be addressed to remain competitive and compliant. From managing complex regulatory requirements to ensuring robust security and efficient operations, payment service providers (PSPs) are navigating an increasingly intricate landscape.

How This Paper Will Help You

By the end of this paper, you will have a clear understanding of the key challenges facing the payments industry and how emerging digital identity technologies can address these issues. This knowledge will equip you to make informed decisions about integrating these technologies into your operations, helping your business stay competitive, secure, and compliant in a rapidly changing environment.

We will explore the following:

1. **Defining the Pain Points:**
   - The first section of this paper identifies and explains the key challenges currently facing the payments industry. These include difficulties in vendor document retrieval, the complexities of onboarding new customers and partners, the persistent threat of fraud, and the increasing demands of regulatory compliance.

2. **Introducing Emerging Digital Identity Technologies:**
   - The second section gives a clear explanation of the digital identity technologies that are emerging as solutions to these challenges, particularly verifiable credentials and digital identity wallets. These technologies offer innovative ways to enhance security, streamline processes, and meet regulatory requirements.

3. How Technology Solves Industry Challenges:

- In the third section, we bring together the pain points and the technological solutions, demonstrating how verifiable credentials and digital identity wallets can directly address the issues of security, speed and regulatory compliance.

4. Expert Insights:

- Next, we'll explore the insights from industry experts who are already implementing these technologies. Their perspectives will provide a real-world view of the challenges and opportunities.

5. Navigating Regulatory Demands:

- Finally, we will examine the regulatory landscape, focusing on four major regulations that are shaping the future of the payments industry. Understanding these regulations is crucial for PSPs to ensure compliance and avoid penalties.

6. A Case Study in Simplicity:

- We'll conclude with a theoretical case study. Laid out in typical form, this case study explores the way a business can address one of the most common issues in the payments industry.

Chapter I.

The Key Pain Points of the Payments Industry

The Key Pain Points of the Payments Industry

Evolving customer expectations, regulatory pressures, and technological advancements naturally drive the payments industry forward. Among the most significant innovations poised to reshape this landscape are digital identity technologies, specifically verifiable credentials and digital identity wallets.

These technologies offer robust solutions to some of the most persistent and challenging pain points faced by the payments industry today. As the industry grapples with the demands of modern transactions—ranging from complex regulatory compliance to the ever-present threat of fraud—digital identity technologies present a way forward that enhances efficiency, security, and customer experience.

In this introductory section, we will explore how digital identity technology addresses key pain points in the payments industry, with a focus on the challenges of merchant document retrieval, ease of onboarding, fraud prevention, and meeting regulatory demands. By examining these areas in detail, we can better understand the transformative potential of verifiable credentials and digital identity wallets in revolutionizing how payment services are managed and delivered.

1.1

Instant Merchant Document Retrieval: A Solution to Communication Headaches

One of the most significant pain points in the payments industry is the process of merchant document retrieval. Whether it’s onboarding a new merchant, verifying compliance with regulatory requirements, or conducting due diligence for a transaction, the process traditionally involves a cumbersome exchange of documents. This often results in a time-consuming cycle of back-and-forth communication between parties, where requests for additional information, clarifications, or updates can lead to delays and inefficiencies.

In the traditional setup, merchant document retrieval is plagued by several challenges, but **the most critically severe scenario is when unredacted personal information is sent by merchants** to payment service providers (PSPs). For instance, a merchant might submit a document containing sensitive payment data, such as the full PAN credit card number, CVC code, or even an image of the physical card itself. In some cases, as seen with certain hotels, merchants may share a guest's full ID number along with their payment details—information that could easily be exploited for identity theft and unauthorized access to banking services.

This practice not only poses serious legal risks, as PSPs are often prohibited from storing or viewing such data, but it also creates logistical challenges in managing and safeguarding sensitive information in compliance with stringent regulatory standards.

Some of the other challenges include:

- **Fragmented Information:** Documents are often scattered across different systems and formats, making it difficult to gather all necessary information in one place.

- **Manual Processes:** Much of the document retrieval process relies on manual efforts, such as sending emails, making phone calls, or filling out forms. This not only slows down the process but also increases the risk of errors and inconsistencies.

- **Lack of Transparency:** Without a standardized method for tracking document requests and responses, there is often a lack of visibility into the status of a retrieval process, leading to frustration and delays.

- **Access control:** Entry-level staff often handle initial document reviews but don't need access to all sensitive information, while risk managers and AML specialists require more detailed access. Balancing these access levels is crucial to prevent unauthorized viewing of sensitive data and ensure compliance.

1.2

Simplifying Onboarding Processes: Enhancing the Ease and Speed of Integration

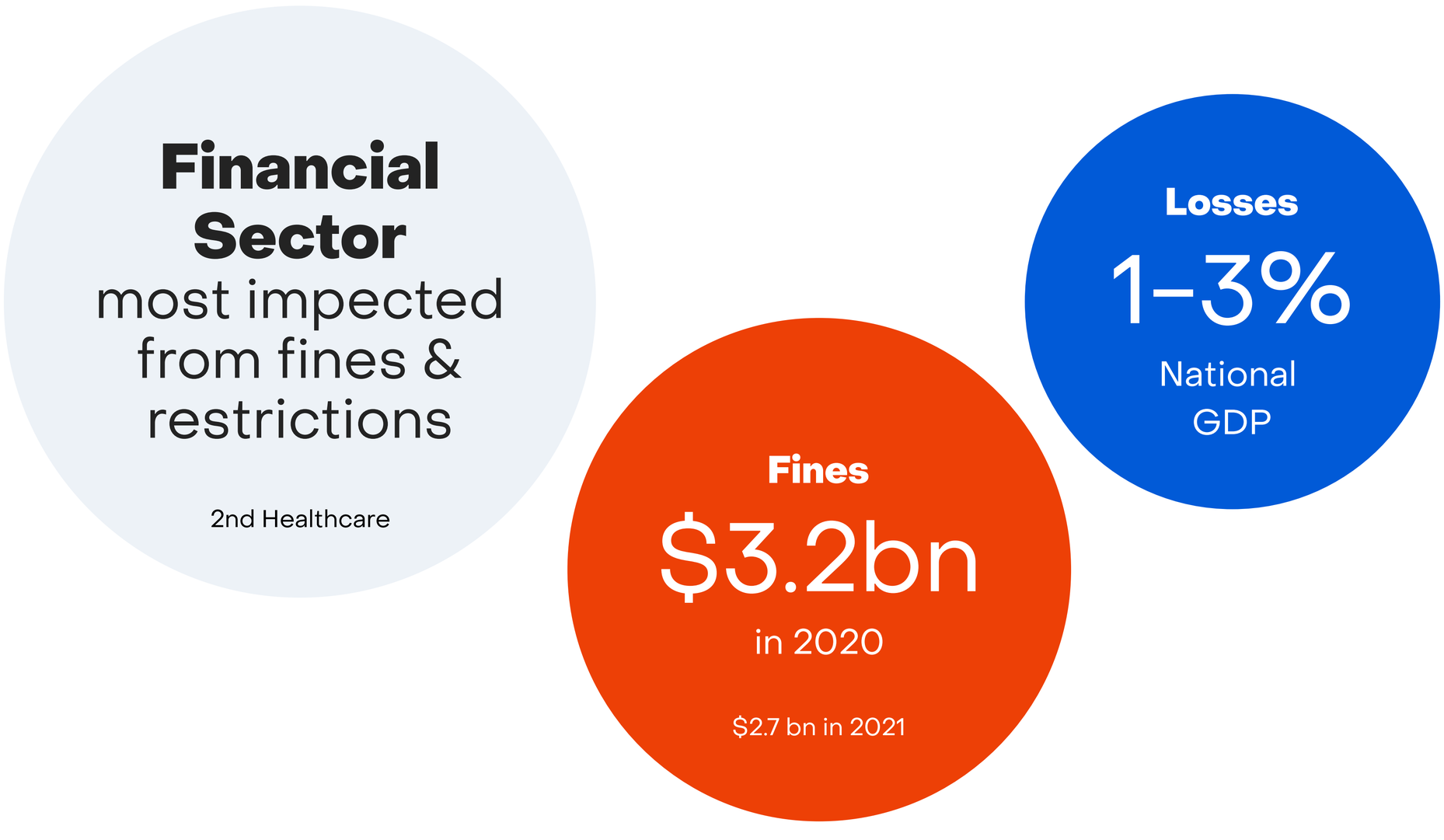
The onboarding process is another critical area where digital identity technology can make a significant impact. Onboarding new customers, merchants, or partners involves verifying their identities, collecting necessary documentation, and ensuring compliance with relevant regulations. In many cases, this process is lengthy and complex, requiring multiple interactions between the PSP and the party being onboarded.

Traditional onboarding processes are often bogged down by several pain points:

- **Multiple Steps and Delays:** The need to collect various forms of identification, financial documents, and compliance records can result in a multi-step process that takes days or even weeks to complete. Each step introduces potential delays, particularly when there are issues with document verification or missing information.

- **Inconsistent Data:** Different parties may provide information in various formats or through different channels, leading to inconsistencies that must be resolved before the onboarding process can proceed.

- **Regulatory Complexity:** PSPs must ensure that all onboarding procedures comply with complex and ever-changing regulations, such as Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements. This adds another layer of complexity to the process, as PSPs must be meticulous in verifying that all regulatory criteria are met.



1.3

Fraud Prevention: Strengthening Security Across Transactions

Fraud is a persistent and growing concern in the payments industry. As digital transactions become more prevalent, fraudsters are employing increasingly sophisticated tactics to exploit vulnerabilities in payment systems. Traditional methods of fraud prevention, such as passwords and manual identity checks, are often inadequate in the face of modern threats.

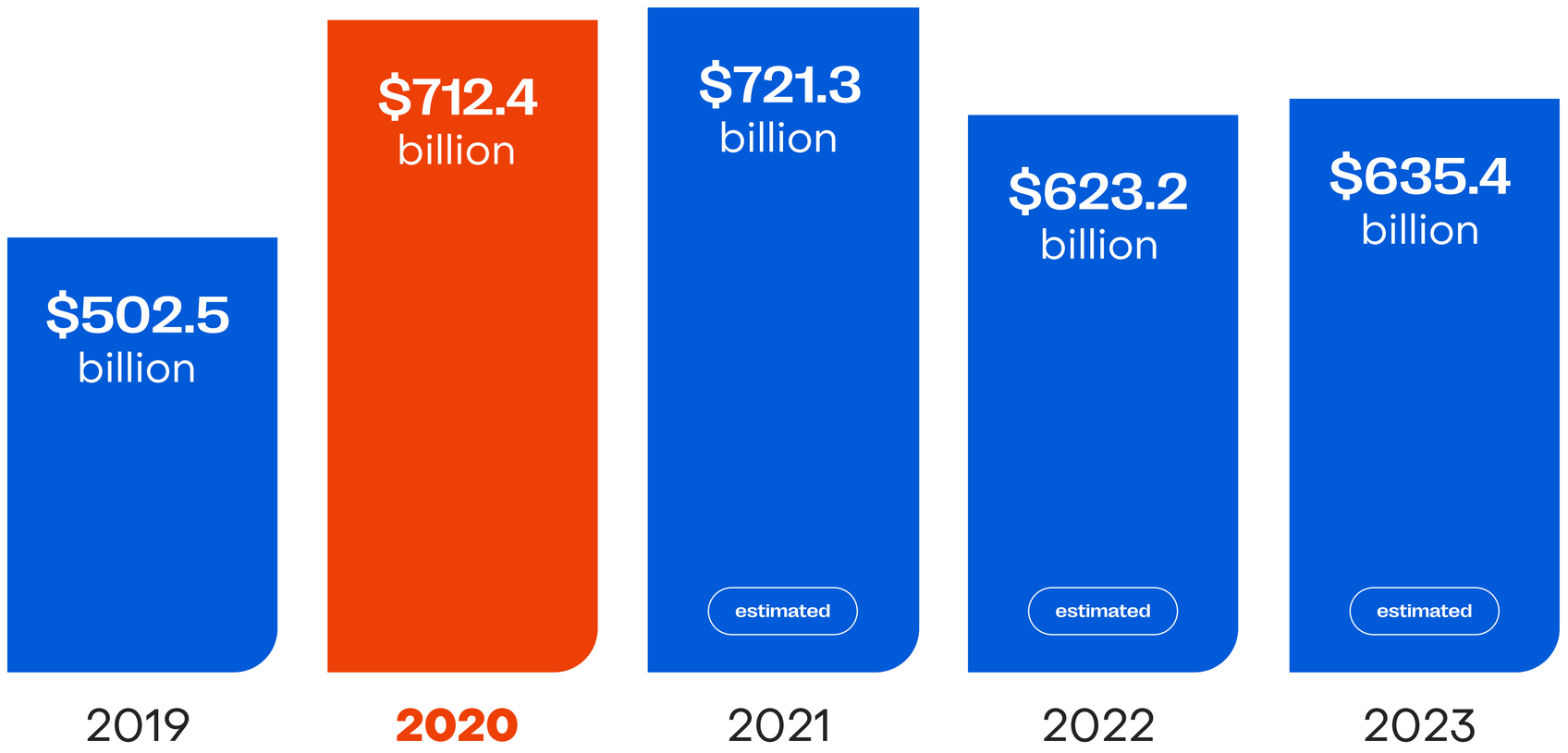
Key pain points in fraud prevention include:

- **Identity Theft and Account Takeovers:** Fraudsters often gain unauthorized access to accounts by stealing or guessing passwords, leading to fraudulent transactions and financial losses.

- **Phishing and Social Engineering:** Attackers use deceptive tactics to trick individuals into revealing sensitive information, which is then used to commit fraud.

- **Inconsistent Security Measures:** Different payment platforms may have varying levels of security, creating weak points that can be exploited by attackers. This is particularly problematic in cross-platform or cross-border transactions.

Losses from Identity Fraud in the US alone reached over $ 712.4 billion in 2020



US firms' losses due to identity theft

Source: Aite Group

1.4

Meeting Regulatory Demands and Enhancing Auditability

The regulatory environment for payment services is complex and constantly evolving. PSPs are subject to a wide range of regulations, including those related to Anti-Money laundering (AML), Know Your Customer (KYC), data protection (such as GDPR), and financial reporting. Ensuring compliance with these regulations can be challenging, particularly when dealing with large volumes of transactions and cross-border payments.

Regulatory pain points include:

- **Complex Compliance Requirements:** PSPs must navigate a myriad of regulatory requirements, often involving detailed record-keeping, reporting, and audits. This can be a significant administrative burden, particularly for smaller PSPs.

- **Inconsistent Data and Reporting:** Ensuring that data is consistent and accurate across different systems and jurisdictions is critical for compliance but can be difficult to achieve. Inconsistent or incomplete data can lead to regulatory penalties or failed audits.

- **Auditing Challenges:** Regulatory audits require PSPs to provide detailed records of transactions, identity verifications, and compliance checks. Gathering and presenting this information can be time-consuming and resource-intensive.

Innovation is Pushing the Payments Industry Forward

Digital identity technologies, particularly verifiable credentials and digital identity wallets, are poised to address some of the most pressing pain points in the payments industry. From streamlining merchant document retrieval and simplifying onboarding processes to enhancing security and fraud prevention and meeting complex regulatory demands, these technologies offer a comprehensive solution to the challenges faced by PSPs. As the payments landscape continues to evolve, the adoption of verifiable credentials and digital identity wallets will be critical for PSPs looking to stay competitive, secure, and compliant in a rapidly changing environment. By embracing these innovations, the payments industry can look forward to a future where transactions are not only faster and more efficient but also more secure, transparent, and customer-friendly.

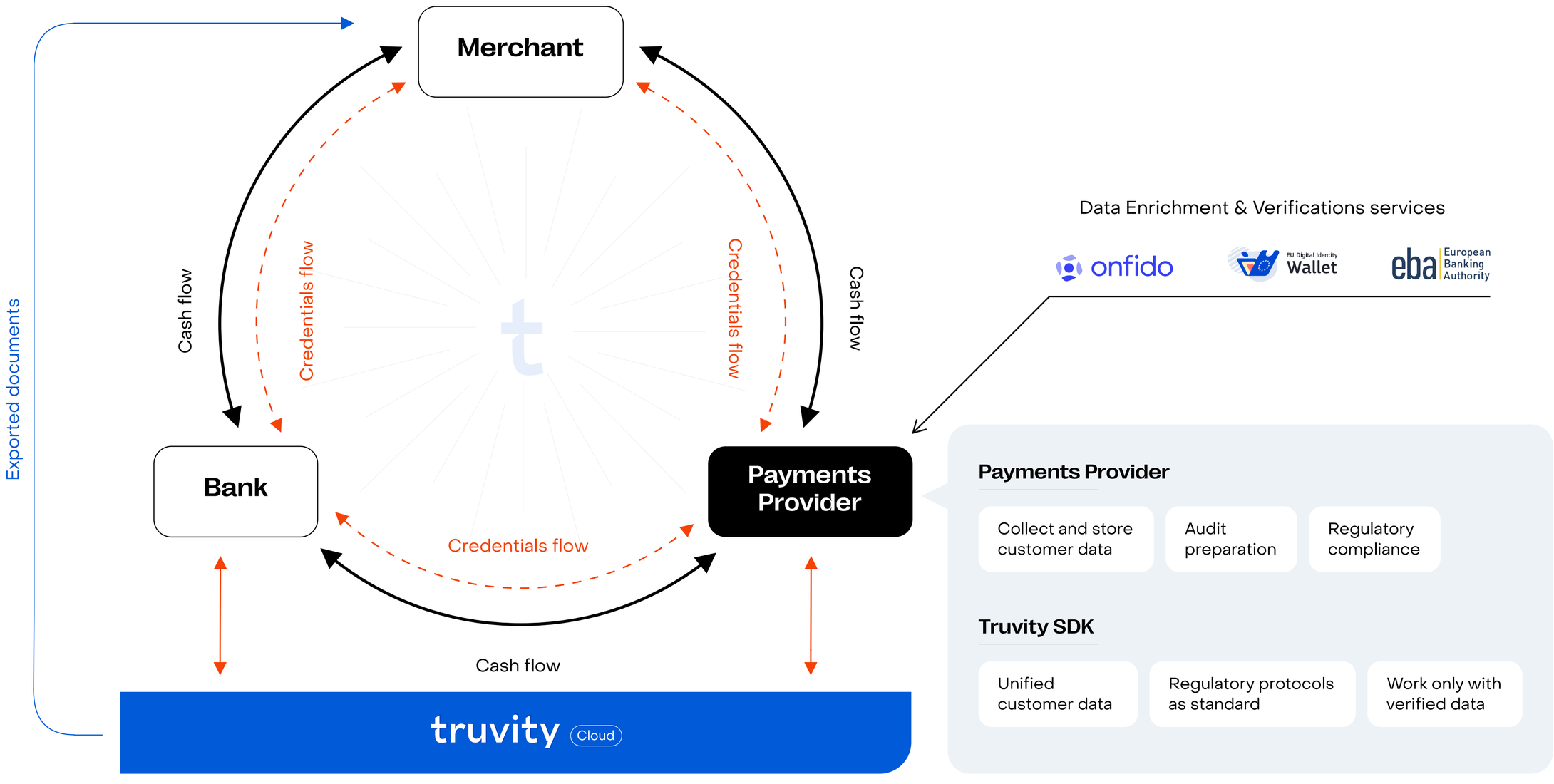
Chapter II.

The Emerging Technologies Helping Solve The Pain Points

The Emerging Technologies Helping Solve The Pain Points

In response to the challenges the industry is facing, the digital transformation in payments is driven by technologies designed to enhance security, streamline processes, and improve customer experiences. Among these innovations, verifiable credentials and digital identity wallets are proving to be particularly impactful.

These tools are poised to solve longstanding challenges in the industry, including identity verification, fraud prevention, and regulatory compliance, while also enabling more seamless and secure transactions.



2.1

What Are Verifiable Credentials and Digital Identity Wallets?

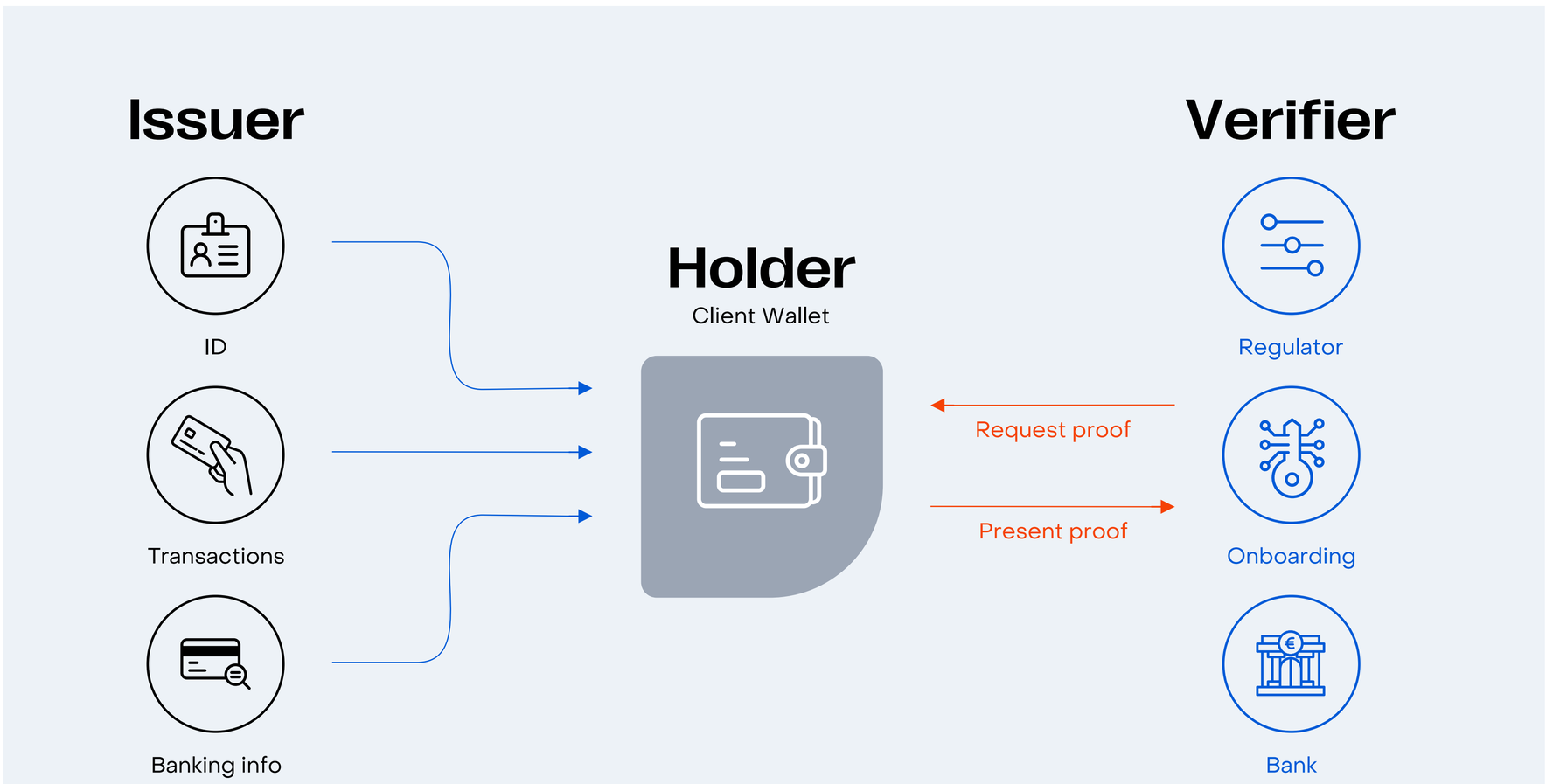
Verifiable Credentials are digital versions of critical documents or qualifications, issued by trusted authorities and designed to be easily verifiable by third parties. These credentials can include everything from identification such as driver's licenses or passports, to payment proofs issued by a business entity, and even proof of regulatory compliance issues by a regulator.

What makes verifiable credentials so significant is their ability to provide secure, tamper-proof verification in real-time, bypassing the need for centralized databases or lengthy verification processes. Unlike traditional verification methods, which often involve multiple intermediaries and risks of data breaches, verifiable credentials enable peer-to-peer verification, significantly enhancing both the privacy of individuals and the security of sensitive information.

One of the key benefits of verifiable credentials is their versatility. They can, for example, streamline compliance processes by enabling secure sharing of regulatory documents between merchants, PSPs, and regulatory authorities. By storing verifiable credentials digitally, businesses can instantly provide proof of compliance, reducing the need for repeated document exchanges and mitigating the risk of errors or fraud. For individuals, verifiable credentials empower them to control their own identity information, sharing only what is necessary and relevant in a secure, trusted manner.

Digital Identity Wallets complement verifiable credentials by serving as secure apps where individuals and businesses can store, manage, and share these digital documents. These wallets provide a user-friendly solution for managing digital identities, giving users full control over their data and who can access it. With a digital identity wallet, businesses can collect and store various credentials—such as proof of identity, the proof or authorisation of payment information, or professional licenses—in one secure location, and then seamlessly share them with third parties as needed. This not only simplifies processes like onboarding and compliance checks, but also enhances trust between businesses and their customers by ensuring that personal data is managed securely.

The integration of verifiable credentials with digital identity wallets provides a secure, all-in-one solution for managing digital identities. This eliminates the need for traditional, centralized verification methods, lowering the risk of data breaches and privacy violations. By allowing users to share only specific pieces of information, digital identity wallets minimize the exposure of sensitive data, further enhancing privacy and security



A verifiable credential is issued by yourself, your business, or a trusted third party. It is then held by a business or individuals and verified on request when interacting with a service provider, regulator or counterparty. The request is for verification specifics and what information is needed, the rest is automated for you.

2.2

Addressing the Key Industry Pain Points with Verifiable Credentials and Digital Identity Wallets

A. Merchant Document Retrieval

Vendor document retrieval has traditionally been a cumbersome process, often involving repeated requests and back-and-forth communication. Verifiable credentials and digital identity wallets simplify this by securely storing all necessary documents in one place.

- **Centralized and Secure Storage:** Merchants can keep all their important credentials, such as business licenses and tax documents, in a digital identity wallet. This allows them to grant instant access to these documents when requested, eliminating delays and unnecessary communication.

- **Instant Verification:** These credentials are digitally secured, allowing for real-time verification without the need for external checks or additional proof. This not only speeds up the process but also reduces the risk of errors or fraud.

- **Transparency and Accountability:** Every action involving verifiable credentials can be logged and audited, creating a clear record of when and how documents were shared. This builds trust between merchants and PSPs by ensuring transparency and accountability.

By addressing document retrieval challenges in this way, PSPs can reduce administrative burdens and enhance the overall experience for merchants, making compliance and business operations smoother and more efficient.

B. Simplifying Onboarding

Onboarding new customers or partners can be a complex and time-consuming process, often hindered by manual verification steps and inconsistent data.

- **Single-Click Onboarding:** With digital identity wallets, individuals and businesses can store all their necessary credentials in one location. When onboarding with a PSP, they can share these credentials directly from their wallet, streamlining the process to just a few clicks.

- **Real-Time Verification:** Verifiable credentials can be instantly confirmed, removing delays caused by manual checks and ensuring that the onboarding process is quick and efficient.

- **Built-In Compliance:** Digital identity wallets can be programmed to automatically ensure that only credentials meeting specific regulatory standards are shared, reducing the risk of non-compliance and simplifying the PSP's responsibilities.

- **Data Consistency:** Because verifiable credentials are standardized, the information shared is consistent and accurate, reducing errors and discrepancies during onboarding.

By simplifying and accelerating the onboarding process, PSPs can offer a more user-friendly and efficient experience, which can help attract and retain customers and partners.

C. Strengthening Security and Preventing Fraud

Fraud prevention is a critical concern in the payments industry. Traditional methods like passwords and manual identity checks are increasingly vulnerable to sophisticated attacks.

- **Eliminating Passwords:** Verifiable credentials replace passwords with cryptographic proofs that are nearly impossible for fraudsters to replicate or steal, significantly enhancing security.

- **Resistance to Phishing:** Since these credentials are digitally signed and verified, they cannot be forged or tampered with, even if intercepted by fraudsters. This makes phishing attacks far less effective.

- **End-to-End Security:** Digital identity wallets provide a secure environment for storing and sharing credentials, ensuring they cannot be accessed or altered by unauthorized parties.

- **Biometric and Multi-Factor Authentication:** These wallets can incorporate biometric methods, such as fingerprint or facial recognition, adding an extra layer of security and ensuring that only the rightful owner can initiate transactions.

By adopting these technologies, PSPs can reduce the incidence of fraud and build trust in their payment services, offering customers a higher level of security.

D. Meeting Regulatory Demands

Regulatory compliance is a complex and ongoing challenge for PSPs, especially when operating across multiple jurisdictions with varying rules.

- **Automated Compliance Checks:** Digital identity wallets can be configured to automatically enforce compliance with relevant regulations, such as AML or KYC, reducing the risk of non-compliance.

- **Real-Time Monitoring and Reporting:** Verifiable credentials provide a clear, auditable record of when credentials were issued, verified, and shared, making it easier to monitor compliance and generate reports for regulators.

- **Simplified Audits:** When audits are required, verifiable credentials and digital identity wallets allow PSPs to quickly gather and present the necessary information in a standardized and easily verifiable format, reducing the time and effort required.

- **Cross-Border Compliance:** These technologies are designed to be interoperable across different jurisdictions, simplifying compliance for global payment providers and ensuring they meet regulatory requirements in multiple countries.

By streamlining compliance processes, PSPs can reduce administrative burdens, lower the risk of regulatory penalties, and enhance the efficiency and transparency of their operations.

Preparing for the Future

As verifiable credentials and digital identity wallets become more widespread, payment service providers need to take proactive steps to integrate these technologies:

- **Upgrade Technology:** Invest in systems that support verifiable credentials and digital identity wallets.

- **Collaborate with Industry Partners:** Work with other financial institutions and technology providers to ensure compatibility and set industry standards.

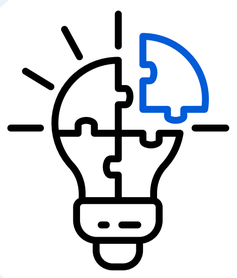
- **Educate Employees:** Train staff on how to use these new technologies effectively, particularly in compliance and customer service roles.

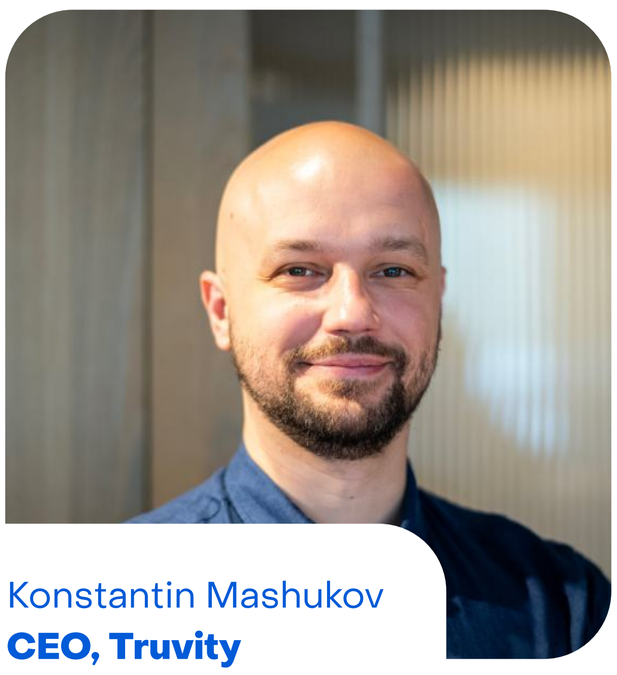
- **Communicate with Customers:** Educate customers about the benefits of these tools to encourage adoption and trust.

- **Monitor Regulatory Developments:** Stay informed about regulatory changes to ensure continued compliance as these technologies evolve.

A Simple Solution to Complex Problems

Verifiable credentials and digital identity wallets offer powerful solutions to some of the most pressing challenges faced by the payments industry. By simplifying document retrieval, streamlining onboarding, enhancing security, and ensuring regulatory compliance, these technologies help PSPs operate more efficiently and securely. As the industry continues to evolve, embracing these innovations will be crucial for staying competitive and delivering exceptional service to customers and partners.





Konstantin Mashukov
CEO, Truvity

"Start and finish payments with trust. Be always informed about who, what, and where you send your payments, and how to make sure nobody is put at risk. New technologies make this once-complex process, simple. Your digital wallet can be the sole source for facts, able to share verifiable information when you need it. No paperwork, no lost emails and no fraud."

Chapter III.

How Changes in Regulation Will Impact PSPs

How Changes in Regulation Will Impact PSPs

The financial landscape within the European Union (EU) has long been shaped by a series of regulatory frameworks designed to foster innovation, ensure security, and enhance consumer protection in the payment services industry. Among these, the Payment Services Directives (PSD) have played a pivotal role in driving the modernization of payment services across the EU. With the advent of PSD3, the latest iteration in this regulatory journey, the industry is once again poised for significant transformation.

The significant transformations in the regulatory landscape don't stop at PSD3 however; as technological progress pushes the financial world forward, additional measures are necessary to address the demands of the future. These changes, driven by the need for greater security, transparency, and efficiency, include eIDAS 2.0, the Markets in Crypto-Assets (MiCA) Regulation, and the Digital Operational Resilience Act (DORA). This blog post will explore these regulations in detail and discuss how they will shape the future of PSPs.

3.1
The Regulatory Landscape Driving the Industry Forward

What is PSD3?

PSD3 represents the European Commission's response to the evolving payments landscape. While the directive is still in its proposal stage, it is expected to build upon the foundations laid by PSD2 while addressing the emerging challenges that have arisen since its implementation. PSD3 aims to enhance competition, foster innovation, improve consumer protection, and ensure the security and resilience of payment systems in an increasingly digital and interconnected world.

Key Objectives of PSD3:

1. **Strengthening Open Banking:** PSD3 seeks to address the inconsistencies in Open Banking implementation across the EU. By refining the rules around API access and ensuring a more harmonized approach, PSD3 aims to create a level playing field for both incumbents and new entrants in the payments market.
2. **Enhancing Consumer Protection:** Consumer protection remains a central focus of PSD3. The directive is expected to introduce stricter requirements for TPPs, including more rigorous licensing and supervision standards. Additionally, PSD3 aims to improve transparency around fees and charges, ensuring that consumers have clear and accurate information when making payment decisions.
3. **Addressing Digital and Crypto Payments:** As digital and crypto payments become more prevalent, PSD3 will likely include provisions to regulate these emerging payment methods. This could involve setting standards for the use of digital currencies, as well as implementing measures to mitigate the risks associated with these new forms of payment.
4. **Bolstering Cybersecurity:** In response to the growing threat of cyberattacks, PSD3 is expected to introduce more stringent cybersecurity requirements for payment service providers. This could include mandatory risk assessments, enhanced incident reporting protocols, and stricter controls around data protection and privacy.
5. **Fostering Innovation:** PSD3 aims to encourage further innovation in the payments industry by promoting the development of new technologies and business models. This could involve creating a regulatory sandbox environment where companies can test new payment solutions under the supervision of regulators.

The Impact of PSD3 on the Payments Industry

As PSD3 begins to take shape, its impact on the payments industry is expected to be far-reaching. The directive will not only introduce new regulatory requirements but also drive significant changes in the way payment services are delivered, managed, and consumed though:

- **Enhanced Competition**

By refining API access and Open Banking, PSD3 will level the playing field, boosting competition and leading to more diverse, competitively priced services. PSPs must innovate and focus on customer experience to differentiate themselves.

- **Stronger Consumer Protection**

PSD3 will raise standards for transparency, security, and service quality. Clearer information on fees and stricter oversight of TPPs will build consumer trust in digital payments.

- **Regulation of Digital and Crypto Payments**

PSD3 will introduce clear rules for digital and crypto payments, ensuring consumer protection and financial stability. This will require adjustments from companies but will provide needed legitimacy to these emerging payment methods.

- **Increased Cybersecurity**

PSD3 will demand stronger cybersecurity measures and regular risk assessments from PSPs. While this requires investment, it will enhance protection against cyber threats and build consumer trust.

- **Fostering Innovation**

PSD3 encourages innovation by supporting new technologies like AI in fraud detection and biometric authentication. PSPs that embrace these changes will be well-positioned in the evolving payments landscape.

eIDAS 2.0: Enhancing Trust in Digital Identities

The original eIDAS Regulation (Electronic Identification, Authentication and Trust Services) was introduced in 2014 to provide a standardized framework for electronic identification and trust services across the EU. It aimed to ensure that electronic transactions could be carried out securely and efficiently across borders. However, as digital transformation has accelerated, the need for a more robust framework has become evident. This has led to the development of eIDAS 2.0.

Key Features of eIDAS 2.0:

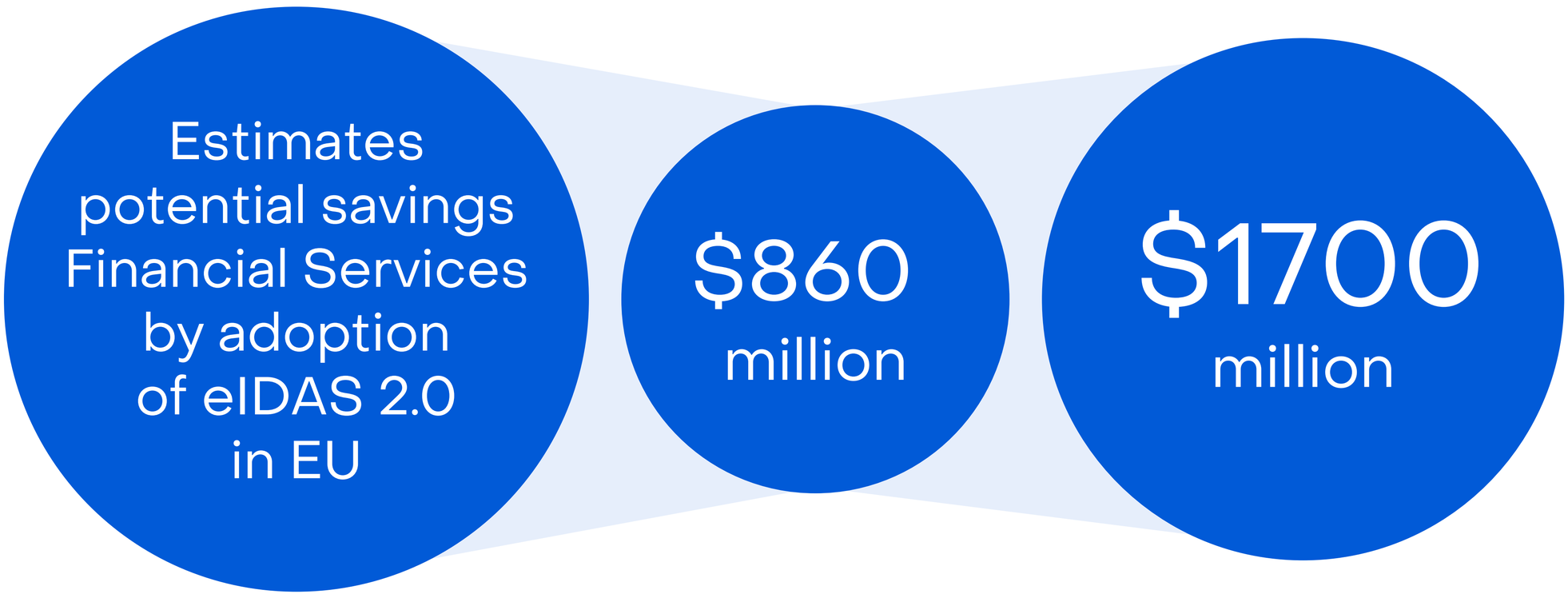
1. **European Digital Identity Wallets:** eIDAS 2.0 introduces the concept of European Digital Identity Wallets. These wallets will allow citizens and businesses to store and manage their identity data and credentials, such as driving licenses, diplomas, and bank accounts, in a secure and user-friendly manner. This feature aims to enhance cross-border digital interactions and reduce reliance on physical documents.

2. **Interoperability:** The regulation emphasizes interoperability between national electronic identification systems. This means that a digital identity issued in one member state must be recognized and accepted in all other member states, facilitating seamless cross-border transactions.

3. **Enhanced Security and Privacy:** eIDAS 2.0 includes stringent security and privacy requirements to protect users' data. This involves the use of advanced encryption technologies and adherence to strict data protection standards.

Impact on PSPs:

For PSPs, eIDAS 2.0 represents both a challenge and an opportunity. The introduction of European Digital Identity Wallets will streamline the process of verifying customer identities, potentially reducing fraud and enhancing trust in digital transactions. However, PSPs will need to invest in upgrading their systems to support the new standards and ensure interoperability with other EU member states' systems.



MiCA: Regulating Crypto-Assets

The Markets in Crypto-Assets (MiCA) Regulation is another significant regulatory development that will impact PSPs. As the popularity of cryptocurrencies and digital assets has surged, regulators have recognized the need for a comprehensive framework to address the associated risks and challenges.

Key Features of MiCA:

1. **Comprehensive Regulation of Crypto-Assets:** MiCA aims to provide a clear regulatory framework for the issuance, trading, and custody of crypto-assets. This includes defining the different types of crypto-assets, such as utility tokens, stablecoins, and asset-referenced tokens, and establishing rules for their issuance and circulation.
2. **Consumer Protection:** The regulation includes measures to protect consumers, such as requiring issuers of crypto-assets to provide clear and detailed information about the assets and associated risks. Additionally, it mandates that service providers implement robust security measures to safeguard consumers' funds.
3. **Market Integrity:** MiCA seeks to ensure market integrity by introducing rules to prevent market abuse, such as insider trading and market manipulation. It also establishes requirements for the registration and supervision of crypto-asset service providers.

Impact on PSPs:

MiCA will require PSPs involved in the crypto-asset market to comply with a comprehensive set of rules and regulations. This will include obtaining licenses, adhering to stringent security protocols, and providing detailed disclosures to consumers. While this may increase compliance costs, it will also enhance the credibility and stability of the crypto-asset market, potentially attracting more customers to PSPs offering crypto-related services.

DORA: Strengthening Digital Operational Resilience

The Digital Operational Resilience Act (DORA) is designed to ensure that financial entities, including PSPs, can withstand and recover from all types of ICT-related disruptions and threats. In an era where cyber-attacks and technology failures are becoming increasingly common, DORA aims to bolster the resilience of the financial sector.

Key Features of DORA:

1. **ICT Risk Management:** DORA requires financial entities to implement robust ICT risk management frameworks. This includes identifying and assessing risks, implementing appropriate controls, and regularly testing and monitoring ICT systems.

2. **Incident Reporting:** The regulation mandates that financial entities report significant ICT-related incidents to relevant authorities. This will help regulators monitor and respond to systemic risks in a timely manner.
3. **Third-Party Risk Management:** DORA emphasizes the need for financial entities to manage risks associated with third-party service providers. This includes conducting due diligence, establishing contractual safeguards, and continuously monitoring third-party performance.

Impact on PSPs:

To comply with DORA, PSPs will need to invest in enhancing their ICT risk management capabilities. This may involve upgrading their technology infrastructure, implementing advanced cybersecurity measures, and conducting regular resilience testing. While this will entail additional costs, it will also help PSPs mitigate the risks of operational disruptions and enhance their overall stability and reliability.

3.2

Navigating the Challenges and Opportunities

The implementation of eIDAS 2.0, MiCA, and DORA presents both challenges and opportunities for PSPs. By understanding and adapting to these regulatory changes, PSPs can not only ensure compliance but also gain a competitive edge in the market.

Investing in Technology Upgrades

One of the primary challenges posed by these regulations is the need for significant technology upgrades. PSPs will need to enhance their systems to support new digital identity standards, ensure interoperability, and implement robust ICT risk management frameworks. This will require substantial investment in technology and cybersecurity infrastructure. However, these upgrades will also position PSPs to offer more secure, efficient, and user-friendly services, enhancing their attractiveness to customers.

Enhancing Customer Trust and Security
Regulatory compliance is crucial for building and maintaining customer trust. By adhering to the stringent requirements of eIDAS 2.0, MiCA, and DORA, PSPs can demonstrate their commitment to security and transparency.

This will not only help mitigate the risks of fraud and cyber-attacks but also enhance the overall customer experience. As customers become more aware of the importance of digital security and privacy, PSPs that prioritize compliance will be better positioned to attract and retain loyal customers.

Leveraging New Opportunities
While the new regulations pose compliance challenges, they also create new opportunities for innovation and growth. For instance, the introduction of European Digital Identity Wallets under eIDAS 2.0 will streamline the process of verifying customer identities and conducting cross-border transactions. This can open up new markets and customer segments for PSPs. Similarly, MiCA's comprehensive framework for crypto-assets will provide greater clarity and stability in the crypto market, encouraging more customers to engage with crypto-related services offered by PSPs.

Collaborating with Regulators and Industry Peers
Navigating the complex regulatory landscape will require close collaboration with regulators and industry peers. PSPs should actively engage with regulatory authorities to stay informed about upcoming changes and seek guidance on compliance requirements. Additionally, collaborating with industry peers can help PSPs share best practices, pool resources, and develop industry-wide standards for regulatory compliance. By working together, PSPs can create a more resilient and secure financial ecosystem.

Building a More Secure Future

The regulatory landscape is undergoing significant changes with the introduction of eIDAS 2.0, MiCA, and DORA. These regulations aim to enhance security, transparency, and resilience in the financial sector. While compliance with these regulations will require significant investment and effort, it will also create new opportunities for PSPs to innovate and grow.

By investing in technology upgrades, enhancing customer trust and security, leveraging new opportunities, and collaborating with regulators and industry peers, PSPs can successfully navigate the regulatory landscape and thrive in the digital era. The journey towards regulatory compliance may be challenging, but it is essential for building a secure, transparent, and resilient financial ecosystem that benefits businesses and consumers alike.

Chapter IV.

A Case Study in Compliance for PSPs with Truvity

A Case Study in Compliance for PSPs with Truvity

The use of digital identity technologies like verifiable credentials (VCs) and other identity technologies is set to revolutionize the payments industry. These allow payment providers and their clients, such as merchants, to streamline processes by securely sharing payment requests and important documents. Merchants can use digital identity wallets to initiate payment requests directly, bypassing traditional, time-consuming verification methods. If banks and other financial institutions also adopt this technology, the entire payment flow could be automated, making transactions faster, more efficient, and more secure.

Beyond speeding up payments, digital identity technology has the potential to enhance security measures such as Anti-Money Laundering (AML) and fraud detection. By integrating identity technologies into their systems, third-party services that provide vital information—like sanction lists—could easily share data, making it more effective to identify risks and prevent fraud.

Digital identity technology also offers major improvements for onboarding and compliance processes. When identity documents are made available through secure digital wallets, payment service providers can automatically verify these documents without relying on third-party services, drastically simplifying customer onboarding. In the future, businesses could fully automate the onboarding process for organizations as well, once critical documents such as proof of business or financial statements are issued digitally by trusted entities. This technology paves the way for a more streamlined, secure, and efficient payments industry.

4.1

The Case Study and Understanding the Compliance Landscape

To illustrate how these can be used to ensure compliance and transparency, an example PSP called Payvity has partnered with Truvity, a leading provider of Full Credentials Lifecycle Management platforms based on Self-Sovereign Identity standards. This collaboration aims to evaluate Truvity's capabilities in meeting Payvity's needs for providing defensible proof of regulatory compliance to all stakeholders involved.

European financial regulations require PSPs to maintain a high level of transparency and traceability in their transaction processes. This includes adhering to stringent Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations, which necessitate sophisticated data management and secure, verifiable credentials. Payvity is committed to ensuring compliance with these regulations, enabling traceability and accountability throughout its transaction processes. This commitment requires an advanced digital wallet capable of managing complex permissions and supporting the latest self-sovereign identity specifications—exactly what Truvity's platform offers.

4.2

The Pilot Implementation

The pilot implementation focuses on testing Truvity's digital wallet capabilities using a hypothetical payment transaction example. This pilot will allow both Payvity and Truvity to align their understanding of the use case and its requirements. The goal is to ensure that payment transactions processed by Payvity are fully compliant with EU financial regulations, maintaining a transparent and traceable transaction history.

5.3

Key Actors and Goals

The primary actors in this use case are merchants and payment gateways.

For instance:

- **Primary Actors:**
  - Merchant-1: Small Business in Germany
  - Merchant-2: E-commerce Platform in France

- **Supporting Actors:**
  - Payment Method-1
  - Payment Method-2
  - Payvity (Credential Wallet Provider)
  - Regulatory Authorities (e.g., European Banking Authority - EBA)
  - Compliance Officer-1

The primary goal of this use case is to ensure that payment transactions processed by Payvity are compliant with EU financial regulations. Secondary goals include maintaining a transparent and traceable transaction history, utilizing self-sovereign credential wallets for secure and verifiable documentation, avoiding legal penalties and sanctions, and enhancing the company's reputation for regulatory compliance and security.

Detailed Workflow

1. **Regulation Familiarization:**
   - Merchant-1 and Merchant-2 review the requirements of EU financial regulations.

2. **Compliance Officer Interviews:**
   - Compliance Officer-1 examines the transaction details and conducts interviews with the merchants to confirm compliance with financial regulations.
   - Compliance Officer-1 issues "Regulatory Compliance Verification Reports" as Verifiable Credentials (VC) to both merchants.

3. **Documentation Collection:**
   - Merchant-1 in Germany and Merchant-2 in France collect necessary documentation, such as transaction records and compliance certificates.

4. Credential Wallets Update:

- Merchant-1 and Merchant-2 upload all non-VC collected documentation into their Payvity credential wallets using Payvity's platform for data remediation when applicable.

5. Verifiable Presentation to Payment Method-1:

- Merchant-1 and Merchant-2 send the compliance information to Payment Method-1 via Verifiable Presentation.

6. Payment Method-1 Documentation Addition:

- Payment Method-1 receives the Verifiable Presentations and adds additional information, such as transaction logs and fraud prevention records, to the compliance documentation.

7. Verifiable Presentation to Payment Method-2:

- Payment Gateway-1 sends the enhanced compliance documentation to Payment Method-2 via Verifiable Presentation.

8. Payment Gateway-2 Documentation Addition:

- Payment Method-2 receives the documentation and adds their additional information, such as transaction processing records and risk assessment reports, to the compliance documentation.

9. Submission to Payvity:

- Payment Method-2 sends the fully documented and verified compliance information to Payvity via Verifiable Presentation.

10. Payvity Compliance Information Addition:

- Payment Method-2 receives the documentation and adds their additional information, such as transaction processing records and risk assessment reports, to the compliance documentation.

11. Submission to Regulatory Authorities:

- Payvity submits the complete regulatory information to the European Banking Authority (EBA) for review and approval. Submitted documents are presented in the required format (e.g., PDF) with metadata included for traceability to the original Verifiable Credentials.

12. Regulatory Review:

- EBA reviews the compliance documentation and confirms compliance with EU financial regulations.

13. Approval and Transaction Processing:

- Upon approval, Payvity processes the transactions, ensuring ongoing compliance and monitoring.

4.4

Addressing Challenges

Throughout this process, several potential challenges may arise.

For instance:

- **Documentation Difficulties:** If the merchants face difficulties in obtaining necessary documentation, Payvity provides support and resources to help them gather the required documents.

- **Information Gaps:** If Payment Gateway-1 or Payment Gateway-2 identifies gaps in the provided information, they request additional documentation or clarification from the merchants before proceeding.

- **Non-Compliance Issues:** If the EBA identifies any non-compliance, Payvity works with the payment gateways and the merchants to address the issues and resubmit the compliance documentation.

4.5

Stakeholder Concerns

Each stakeholder in this process has specific concerns:

- **Merchants:** Ensuring they have the resources and support to gather and upload the necessary compliance documentation.

- **Payment Methods:** Managing the integration and verification of compliance information while maintaining transaction efficiency.

- **Payvity:** Ensuring that all transactions meet regulatory requirements and that compliance information is accurate and credible.

- **Regulatory Authorities:** Ensuring that the transactions comply with EU financial regulations and maintaining the integrity of the regulatory process.

- **Compliance Officer-1:** Ensuring accurate and unbiased verification of regulatory compliance through merchant interviews.

4.6

A Natural Collaboration

This hypothetical collaboration between Payvity and Truvity highlights the importance of advanced digital solutions in ensuring regulatory compliance within the European financial industry.

By leveraging Truvity's self-sovereign identity platform, Payvity can provide a secure and user-friendly solution for managing and sharing compliance documentation, ultimately enhancing their reputation for regulatory compliance and security. This pilot implementation serves as a critical step towards achieving a transparent, traceable, and compliant transaction process in the ever-evolving landscape of European financial regulations.

Chapter V.

Wrapup and Final Thoughts

As the payments industry continues to evolve, the challenges faced by payment service providers (PSPs) are becoming increasingly complex. By integrating emerging technologies into your operations, you can not only tackle the current pain points in the industry but also position your business for future success. The insights and strategies discussed in this document highlight the critical role that digital identity solutions will play in shaping the future of payments.

To stay competitive and prepared for the future, we encourage you to explore how Truvity can help. Our Access Program is designed to support your adoption of these technologies through free consulting, direct support from our CEO and free access to our API/SDK to get started. Ensure your business is ready to meet the evolving demands of the payments industry. Join us and let Truvity guide your success.

Konstantin Mashukov
CEO

k.mashukov@truvity.com

George Fisher-Wilson
Head of Marketing

g.fisherwilson@truvity.com