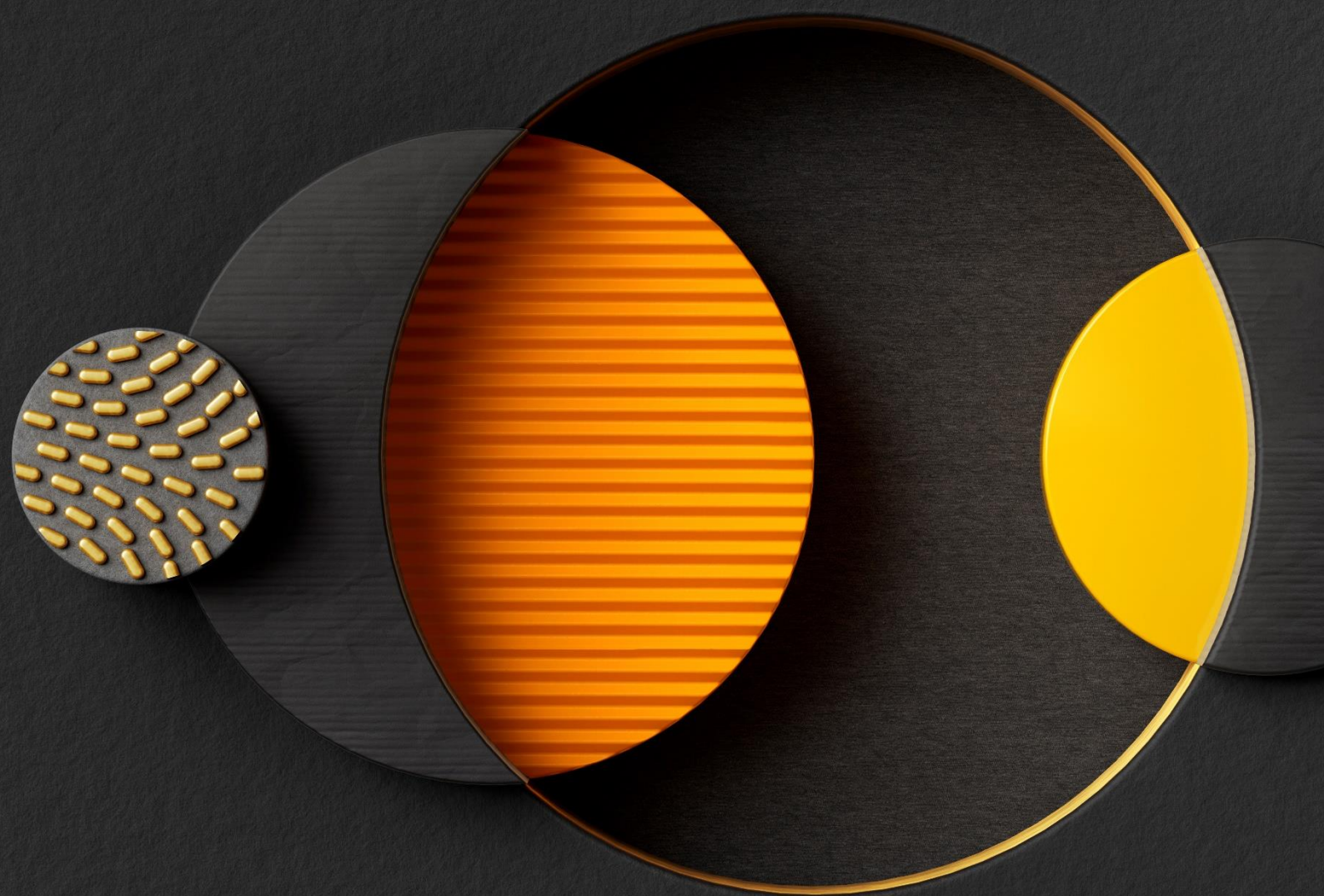


Financial Sector & Resilience



Stories of Innovation, Security & Regulation
and their impact on economic resilience in
Slovenia and beyond



Published in 2025 by Mastercard Europe SA, Slovenia Branch with the consent of all contributors to the publication.

All views expressed by all contributors are their own and do not necessarily reflect the official views of the organization they represent.



Foreword

Resilience in the financial sector is no longer defined solely by capital buffers or liquidity ratios – it is increasingly shaped by the sector's ability to innovate, adapt, and anticipate. In Slovenia, innovation is gradually transforming the financial landscape, from digital banking services to fintech collaborations. Yet, the pace of digital transformation still lags behind the euro area average. This presents both a challenge and an opportunity: by accelerating innovation – particularly in areas like green finance, open banking, and AI-driven risk management – Slovenian institutions can enhance their operational agility and better withstand future disruptions.

Cybersecurity has become a cornerstone of resilience, particularly in the realm of digital payments. As Slovenia's financial institutions and consumers increasingly embrace electronic transactions, the need for robust protection against cyber threats has intensified. The implementation of the EU's Digital Operational Resilience Act (DORA) is helping to standardize ICT risk management across the sector, ensuring that banks, insurers, and payment service providers meet stringent security and incident reporting requirements. However, resilience in digital payments also depends on the integrity and reliability of the broader ecosystem – including international card schemes, which remain the backbone of our collective cyber defence. Strengthening cybersecurity across all layers of the affected digital ecosystems through technology, data, appropriate incentives and underlying partnerships is essential to ensuring that the financial sector stays resilient.

Regulation is another key element of systemic resilience. Slovenia's macroprudential policy continues to play a preventive role in safeguarding the financial system against both domestic and external shocks. Regulatory instruments have helped maintain stability amid rising geopolitical tensions and economic uncertainty. As the sector navigates evolving risks, including climate and cyber threats, regulatory agility will be essential. The challenge lies in balancing oversight with flexibility, enabling institutions to innovate while remaining secure and compliant.

This collection of essays and articles offers a timely reflection on how innovation, cybersecurity, and regulation intersect to shape the resilience of Slovenia's financial sector. It invites readers to consider not only the technical dimensions of resilience but also the strategic choices that will define the sector's future. As Slovenia continues its journey toward a more digital, secure, and sustainable financial system, the insights gathered here aim to inform, inspire, and provoke meaningful dialogue across policy, industry, and academia.



Luka Gabrovšek

Mastercard, Country Manager for Slovenia



Contents

Innovation.....	6
Shaping the Future of Payments: Tokenization and AI in Europe	7
Digital transformation in Slovenia	12
Blockchain and Crypto: Enhancing Financial Resilience through Innovation and Regulation.....	15
Empowering European Businesses and Consumers Through Digital Payments	18
Cybersecurity	20
Mastercard's commitment to cybersecurity	21
Information Security as a Social Responsibility: The Need for Lifelong Awareness	23
Security challenges and opportunities for banks.....	25
TTP Framework: A Structured Approach to Understanding and Countering Cyber Threats	28
Regulation	30
Open Strategic Autonomy: international collaboration, sound regulatory oversight and innovative legal frameworks.....	31
Strengthening Economic Resilience through a Competitive Taxation System	34
Regulatory considerations for the improvement of the Slovenian banking sector.....	37
Roadmap towards a resilient, prosperous, and liveable Europe	40

Innovation



Shaping the Future of Payments: Tokenization and AI in Europe

by Arne Pache, Mastercard, SVP, Customer Solutions Center, Central Europe

Europe's digital commerce is booming, but friction and fraud still plague the checkout. In fact, studies predict roughly 70% of online shopping carts will be abandoned in 2024 due to hassles like security concerns and lengthy forms¹. To solve this, Mastercard and its partners are pushing a radical overhaul: phasing out manual card entry by 2030 in favour of one-click, tokenized payments and AI-driven "agentic" commerce². In this vision, consumers pay with a single tap or even via an AI assistant, while all sensitive data is hidden behind dynamic tokens and strong authentication. Recent announcements and pilots show this is far more than theory – it's the next frontier of European payments.



Mastercard's Tokenization: Security and Seamlessness

Mastercard has pioneered tokenization – replacing the 16-digit card number with a one-time random token – as a cornerstone of its strategy. This approach, standardized by EMVCo in 2013, ensures that "your actual card information is never transmitted" in a transaction³. Tokens are bound to specific devices or merchants, so even if stolen, a token by itself is worthless. The impact has been dramatic: today over 30% of Mastercard transactions globally are tokenized, with "more tokens enabled for digital payments than [there are] physical cards"⁴. That has led to measurable benefits – tokenization reduces e-commerce fraud and improves approval rates, lowering declines by 30% or more in early pilots⁵.

- **Enhanced Security.** Because tokens never expose the real card number, breaches of merchant vaults no longer yield usable data. Fraud attacks on payment networks are cut off at the pass, and one industry report forecasts \$600 million in annual fraud savings from tokenization alone⁶. Meanwhile, all parties – consumers, banks, and merchants – benefit from richer data attached to tokenized payments, enabling machine-learning fraud detectors to spot anomalies faster⁷.
- **Seamless UX.** Tokenization works behind the scenes with no added burden on consumers. Users don't have to update expiring cards: behind-the-scenes systems automatically reissue fresh tokens, keeping subscriptions like Netflix running without a password reset. In practice, cardholders tap or click and go. Mastercard is even integrating on-device passkeys (biometric logins) into checkout, eliminating OTPs or passwords. In short,

¹ dis-blog.thalesgroup.com

² mastercard.com/pymnts.com

³ mastercard.com

⁴ mastercard.com

⁵ mastercard.com/mastercard.com

⁶ businessofpayments.com

⁷ pymnts.com

tokenization delivers “the same security, simplicity and speed to online checkout that contactless has created in the physical world”.

- **New Use Cases.** The tokenization framework now spans far beyond phones. Mastercard notes tokenization is “pervasive” in transit (tapping to ride), retail, wearables, even connected cars and IoT. For example, drivers can “pay at the pump” or tolls automatically via tokenized in-car wallets. B2B commerce is next: Mastercard’s “multi-token network” can automate complex supply-chain payments (e.g. a tokenized corporate card that splits payments across multiple shipments) to boost transparency.

Mastercard’s public targets underline the push: by 2030 100% of e-commerce in Europe will be tokenized, essentially eliminating the need to type card numbers⁸. This echoes CEO Michael Miebach’s plan to scrap static card data from checkout entirely – requiring only a biometric tap or click. Already, the results are convincing: merchants like JustEatTakeaway.com report half the chargeback rate and ~5.5% higher conversions using tokenized one-click pay⁹. The message is clear – more tokens means faster, safer commerce for everyone.

Click to Pay: Simplifying E-Commerce in Europe

Tokenization underpins Click to Pay, Mastercard’s EMVCo-standard “secure remote commerce” checkout solution. Click to Pay lets consumers store cards once with any issuer, then check out anywhere with a single click – without retyping data or passwords. This federated wallet is supported by all major networks (Mastercard, Visa, Amex, Discover)¹⁰, so it looks and feels familiar to shoppers while masking every detail behind tokens. Click to Pay dramatically cuts friction: consumers choose from pre-registered cards on any trusted device, and the merchant receives only the tokenized credentials.

In Europe, adoption is accelerating. Mastercard has signed deals to embed Click to Pay across the continent. For example, a landmark partnership with e-commerce platform PrestaShop in 2024 enabled all its merchants in France, Spain, Italy and the UK to offer Click to Pay. This means millions of consumers in the EU’s largest markets can now enjoy one-click checkout. Fintech platforms like Yuno and PSPs like Ecommpay are similarly expanding Click to Pay to dozens of countries, integrating it into global payment flows¹¹. Even as customers rely on emerging solutions like Apple Pay or PayPal, both Mastercard and Visa are mandating issuers to support Click to Pay: by 2025 they expect every bank in every country to offer it.

Click to Pay is already showing results. It reduces cart abandonment (eliminating data-entry at checkout), and networks report that Click to Pay transactions “more than doubled” year-over-year as merchants roll it out¹². Issuers see higher approval rates and 40% lower fraud on Click-to-Pay orders¹³. Because Click to Pay payments are tokenized end-to-end, they also satisfy EU Strong Customer Authentication (SCA) requirements while remaining user-friendly. The Thales Payments

⁸ pymnts.com

⁹ mastercard.com

¹⁰ mastercard.com

¹¹ y.unobusinessofpayments.com

¹² businessofpayments.com

¹³ dis-blog.thalesgroup.com

Association notes that with Click to Pay (and supporting passkeys), “the dawn of agentic commerce” – a truly frictionless checkout – is at hand.

Key advantages of Click to Pay in Europe include:

- **Faster checkout:** One-click purchases without retyping billing, shipping or card details.
- **Cross-border consistency:** An EMVCo standard wallet works across all supported sites and devices, reducing ‘cart drop’ in multi-country shopping.
- **Higher security:** Built on tokenization and network-level security, it avoids weak passwords and offloads PCI scope from merchants.
- **Merchant integration:** Click to Pay “integrates smoothly” with existing checkout pages and is often cheaper to deploy than proprietary wallets.

By merging Mastercard’s token platform with Click to Pay’s user-centric design, Europe is seeing a quiet revolution: payment flows are becoming as effortless as using contactless cards. Real-world pilots (e.g. Checkout.com with tokenized credentials) report “reduction in fraud really helping [merchants] grow”. In sum, Click to Pay is raising the bar for e-commerce UX and is on track for near-universal rollout in the EU.

Agentic Pay: AI at the Helm of Transactions

Beyond one-click, the next frontier is agentic pay – payments initiated by AI agents on behalf of users. The idea: users delegate routine purchases to an intelligent assistant, who then shops, negotiates, and pays automatically. This goes far beyond today’s voice assistants or chatbots. Mastercard’s new “Agent Pay” program, launched April 2025, exemplifies this vision¹⁴. Agent Pay introduces “Mastercard Agentic Tokens” – essentially tokenized credentials built for AI commerce – and it weaves them into generative AI platforms to “deliver smarter, more secure, and more personal payments experiences”.

How would this work? Imagine a consumer planning a birthday party. Instead of browsing retailers, she tells an AI agent her style and budget. The AI scans local boutiques, picks products, and initiates the checkout by invoking her stored Mastercard credential – all in one conversational thread. Behind the scenes, Agent Pay uses the same tokenization backbone: the agent grabs a virtual card token (e.g. Mastercard One Credential), the network recognizes the token and the user’s verified account, and the purchase completes with no human key entry. Similarly, small businesses could employ AI agents to handle procurement: sourcing a supplier, negotiating price, and instantly paying via a tokenized virtual corporate card.

The promise of agentic pay is truly frictionless automation: payments become an invisible part of intelligent workflows. Analysts foresee a \$50 billion AI agent economy colliding with a \$37 trillion digital-payments market¹⁵. Mastercard’s program partners with Microsoft (Azure OpenAI) and IBM

¹⁴ [mastercard.com](https://www.mastercard.com)

¹⁵ thepaymentsassociation.org

(Watson) to scale these use cases¹⁶. Already, initiatives are underway: banks and tech firms are integrating AI “copilots” that can pay bills, rebalance portfolios, or even schedule routine orders, all using registered tokenized credentials.

However, agentic pay will only succeed if trust is built in.

Mastercard’s launch details emphasize new guardrails. Agents must be pre-registered and verified before making payments, ensuring that each AI assistant has a unique, auditable identity. Consumers retain full control over agent permissions – deciding exactly what the agent can buy. Each agentic transaction is tagged by the network so that banks and merchants can distinguish AI-driven orders from normal ones. In other words, while AI does the heavy lifting, tokenization and crypto-grade security keep it in check. “Mastercard is transforming the way the world pays by anticipating consumer needs on the horizon,” says CPO Jorn Lambert – noting that Agent Pay is about “distinguish[ing] trusted agents from bad actors” and establishing the protocols that “lay the foundation for scale and build trust in agentic commerce.”.

Key Agentic Pay points:

- **Personalization:** AI agents can tailor purchases (best brands, prices, delivery) and then pay instantly via tokens.
- **Device agnostic:** Any conversational interface (voice, chat, app) can initiate a tokenized transaction, making payments as easy as speaking.
- **Security:** Agent Pay uses the existing token network (plus passkeys/biometrics) and mandates agent verification to prevent fraud.
- **B2B automation:** AI agents can automate complex business transactions (cross-border orders, compliance checks, escrow payments) with programmable virtual cards.

By integrating AI with tokenization, agentic pay could dramatically redefine the user journey: the consumer or business owner simply tells an app or smart speaker what they need, and the rest happens behind the scenes. This is a visionary step, but the building blocks are falling into place thanks to Mastercard’s and others’ early initiatives.

Looking Ahead

The convergence of tokenization and AI-driven payments promises a future where Europeans transact with unprecedented ease and confidence. By eliminating passwords and card numbers, one-click checkout can feel as natural as tap-and-go, and by harnessing AI agents, routine purchases can happen silently in the background, freeing users to focus on what they value. Key statistics underscore the opportunity: Mastercard’s tokens have already grown 49% year-on-year¹⁷, and industry forecasts show trillions in untapped growth from smarter payments. Real-world trials (like Pay by Bank in the Netherlands, QR codes in Scandinavia, or voice shopping pilots) hint at what’s to come.

It’s time for businesses, banks and policymakers to **join the journey**. The technologies are maturing now: token vaults and AI platforms exist, and standards (EMVCo, Model Context Protocol, SCA

¹⁶ electronicpaymentsinternational.com

¹⁷ businessofpayments.com

frameworks) are evolving in parallel. Collaboration is the way forward – between tech giants and startups, regulators and banks. The European payments industry should capitalize on these innovations as strengths: a unique blend of stringent security and cutting-edge UX. In an era of rising cyber threats, tokenization and agentic commerce are not just luxuries – they are necessities to protect consumer trust.

As Mastercard's vision suggests, the eventual payoff will be a seamless, global checkout where **security is invisible**, and the payment is done before the shopper even reaches for her wallet. That future is within reach in Europe – if we embrace these advances.

Digital transformation in Slovenia

by Nena Dokuzov, Ministry of the Economy, Tourism and Sport

Slovenia was the first country globally adopting strategic Action plan for development of blockchain technology and developing the regulatory environment for blockchain applications in 2018. In that period Slovenia was announced as one of the most advanced countries in the field of blockchain technology and innovation. There were large investments in the innovative use cases, either based on crypto or pure blockchain technology and its application in various domains. For first time there was larger share of private investments in blockchain applications comparing traditional funding from institutional investment.



As technology developed and there was even stronger ambition to showcase the successful application of advanced digital technologies, the convergency of those technologies was extremely important for the further developed innovative projects and initiatives.

Slovenia adopted the Strategy for digital transformation at the beginning of 2022. It was one of the most advanced strategies on the EU level. It covers three main pillars: advanced digital technologies, three most important ecosystems (entrepreneurial, research, development and innovation and financial ecosystem, regulatory and social component of digital transformation.

The Strategy defined Slovenia's Vision and the mission in the field of fast adoption of advanced digital technologies.

Vision: By 2030, Slovenia will have become the leading hub of advanced digital technologies in Europe.

Mission: Slovenia's mission in the digital transformation of the economy is to enhance efficiency and productivity, competitiveness and resilience of Slovenian companies by simultaneously increasing the use of advanced digital technologies and ensuring sustainable transformation effects by strengthening knowledge and digital competences, developing digital public services, supporting the collaboration of companies at the international level and exploiting the advantages of the new digital environment in an inclusive and just way.

Objectives

Preserving and strengthening the leading role in advanced digital technologies

Automation and robotization

Artificial Intelligence

Internet of Things

Data and data analytics

Blockchain

Quantum computing

Ensuring a stable and developing environment for the economy's growth and strengthening society through digital transformation

Stable and development-oriented supportive environment

Digital infrastructure

Knowledge, competences and social inclusion

Systems and innovative regulatory environment

International inclusion

The Strategy was also a reform element as recovery measure after the pandemics COVID19. It was not only the basis intended to push the application of advanced digital technologies but created a path for digital transformation of the economy as such. It enabled digital transformation of large companies, which in collaboration with SMEs and innovative startups contributed to digital transformation and consequently to more efficient and resilient businesses in several industrial verticals. And for the first time, the government with its measures caused a spillover effect and motivated large Slovenian companies (like Telekom Slovenia, commercial banks – NLB) to create instruments with the purpose to support digital transformation of SMEs.

The strategy was also a motivating element for Slovenia to enter into strong European integrated projects in the industries which were indicated as the most important areas for strategic autonomy and more resilient European economy: Important projects of common European Interest (IPCEI). The importance of those project lies in the fact that it requires collaboration of the companies on the European level, in the fields of experimental research and industrial development, including first industrial deployment. As the pre-condition is collaboration, the main objective to bring innovative solutions beyond-state-of-the-art. As all IPCEIs are based on the development of the solutions using advanced digital technologies, they act as a motivator to boost digital innovation as well.

Slovenia is participating in the IPCEI-s on cloud-edge continuum, dedicated to strengthening digital infrastructures and connectivity on the European level, while ensuring decentralized, distributed and federated approach. The second IPCEI Slovenia is a part of is on microelectronics and telecommunications. As there is a need for strengthening innovation and competitiveness also with

regards to alternative energy resources and renewables, we joined IPCEI on batteries and in the later stage IPCEI on hydrogen technologies and their industrial use. One of the more important IPCEI we also participate in is IPCEI in the field of health, focused into advanced medical devices, imaging and personalized medicine, with the extensive use of AI solutions.

Mario Draghi pointed out in his report on the competitiveness of Europe the strong importance IPCEI for better efficiency and competitiveness of European economy to catch up other developed regions and narrowing the gap of lagging behind in the field of innovation, development and market shares of European companies. Therefore, there have been developed or in the development phase next IPCEIs, in the field of AI continuum, connected digital infrastructures, advanced semiconductor technologies, circular advanced materials, nuclear technologies. Slovenian companies are recognized as contributors to beyond-state-of-the-art solutions of these European integrated projects.

Slovenia was also one of the most recognized EU projects funded from Digital Europe Program. We actively participated in the creation and development of the project based on blockchain technology focusing on the traceability of data, documents, materials and products, aiming to create a common reference architecture as a standard and common framework for traceability.

We also co-created the next use case on blockchain, project on self sovereign identity, in which the recent modification of eIDAS regulation were addressed. A concept of digital identity of the enterprises was developed and corresponds to the solutions of EU Digital Identity wallet (EUDIW). This solution has a potential not only to simplify the processes of the companies on the national level, but also, taking into account decentralized and distributed nature of blockchain, better access to the European market, visibility and recognition, but also access to finance, either institutional or private, venture capital investment.

As on the EU level there was adopted the regulation on DLT pilot regime, which enables the creation of tokenized financial instruments or to tokenize existing financial instruments, it opens even further better access to funding for startups and small and medium sized companies. As the objective of better access to alternative sources for SMEs and startup companies was one of the main objective of the Strategy of the development of capital market in Slovenia, there was a study developed by the Ministry of finance on mapping the legal basis and potential modifications of them to enable implementation of DLT pilot regime.

This action goes hand in hand with the development of the Slovenian startup strategy, being in preparation by the Ministry of economy, in collaboration with the startup community, which identifies 5 key areas to boost the innovative startups and can contribute to scale up phase in the future. Key areas are: excellent supporting environment, attractiveness for global talents, venture capital investments, options as incentives for employees and a new type of legal entity based on tokenized digital presentations of investment and funding mechanisms.

The ambition is to even more simplify the establishment of the startup companies with high innovation potential, even if Slovenia is one of the most advanced countries when it comes to the time and procedures of starting the business in simplified way. It will also enable faster raising of capital needed in the scaleup phase. And it will open the door for private venture capital investors to bring even more fuel into Slovenian and European economic growth.

Blockchain and Crypto: Enhancing Financial Resilience through Innovation and Regulation

by Miha Goriup, Paywiser, Chief Legal Officer

Blockchain technology and cryptocurrencies are transforming and revolutionizing the financial sector, enhancing economic resilience through decentralized systems, robust security, and innovative financial instruments like stablecoins, tokenized deposits and Decentralised Finance (DeFi). By leveraging distributed ledger technology (DLT), blockchain offers a robust framework that enhances efficiency while fostering trust, allowing for optimisation of payments and transfers of value among other things. The regulatory landscape, exemplified by the EU's Markets in Crypto-Assets (MiCA) Regulation and recently adopted U.S. GENIUS Act, plays a critical role in balancing innovation with stability. As the financial sector navigates economic volatility, these technologies offer robust solutions, but their potential hinges on balanced regulation that nurtures innovation while ensuring stability.



Blockchain's decentralized architecture is a cornerstone of financial resilience. Unlike centralized banking systems, vulnerable to cyberattacks or institutional failures (e.g., the 2008 financial crisis), blockchain distributes data across a network of nodes, ensuring operational continuity through advanced Consensus Mechanisms (Proof of Work or Proof of Stake). Stablecoins, issued on Blockchain technology have the ability to transform money through its defining traits: decentralization, immutability, transparency, and security, making stablecoins a compelling alternative to bank money. During the 2022 FTX collapse, blockchain's transparency enabled users to track assets on-chain, mitigating losses compared to opaque centralized systems. DLT's immutability and cryptographic security further enhance trust, with transaction records being tamper-proof and publicly verifiable. This resilience is even more critical in volatile economies, where traditional systems often falter.

Stablecoins (US) or e-money tokens (EU),
cryptocurrencies pegged to fiat currencies, are a
standout innovation, already revolutionizing
cross-border payments.

Unlike SWIFT, which processes transactions in days with high fees, stablecoins settle globally in seconds at a negligible cost. In 2024, stablecoins facilitated \$27 trillion in on-chain transactions, surpassing Bitcoin's \$19 trillion, with USD-backed stablecoins like Tether (\$170 billion USDT issued) and Circle (\$70 billion USDC issued) dominating 60% of crypto transaction volume. Euro-based stablecoins, such as Circle's EURC and Société Générale's EURCV, are slowly gaining traction under MiCA's regulatory clarity. One thing is already clear, by reducing reliance on intermediary-heavy systems, stablecoins enhance financial inclusion and resilience, offering a convenient new way of transferring money and transacting globally.

The regulatory landscape is pivotal in harnessing blockchain's potential. The EU's MiCA, fully effective as of December 2024, standardizes rules for crypto-asset service providers and e-money token issuers, mandating 1:1 liquid reserves and robust anti-money laundering compliance. This has boosted investor confidence, attracting traditional institutions to crypto markets. However, MiCA's high compliance costs and exclusion of decentralized finance (DeFi) protocols risk stifling some innovators, potentially ceding technological leadership to less-regulated jurisdictions. In the U.S., the recently adopted GENIUS Act aims to integrate stablecoins into the financial system by licensing issuers and requiring transparent reserve disclosures. With 80% of USD stablecoin flows occurring outside U.S. borders, the act seeks to maintain global dollar dominance while fostering innovation.

For the EU, scaling euro stablecoins and tokenized deposits (bank deposits recorded on DLT with programmable features) is of strategic value and critical to challenge USD stablecoin dominance (\$285 billion USD vs. \$0.6 billion for EUR). Tokenized deposits, still in pilot phases (e.g., ING, DWS), offer real-time settlement, enable interest payments and deposit protection under schemes like the EU's Deposit Guarantee Scheme, reducing counterparty risk. These instruments drive innovation through programmable smart contracts, enabling automated lending and trade finance solutions, which enhance liquidity during crises. An innovative euro stablecoin could boost the EU's global trade relevance, reducing reliance on USD infrastructure and reinforcing monetary sovereignty.

To maximize blockchain's contribution to financial resilience, regulators must adopt a balanced approach.

Overly strict rules, like MiCA's high compliance costs, risk stifling innovation. MiCA's exclusion of decentralized finance (DeFi) from its scope leaves gaps in regulating emerging blockchain applications, potentially undermining resilience if risks in these areas go unaddressed. Decentralized Finance (DeFi) has the ability to further transform financial systems

by enabling actions like lending, borrowing, liquidity provision, yield farming, staking, trading, and tokenized asset investment using crypto assets (e.g., stablecoins like USDC, EURC) on different blockchains like Ethereum and Solana. Unlike fiat currencies in banks, which offer limited actions (savings, loans, payments) through centralized systems with low interest rates (0.1–4% APY), DeFi provides permissionless access, yielding 2–20% APY via protocols like Aave (lending), Uniswap (liquidity), and Lido (staking). Consumers control their crypto assets directly via private wallets, bypassing bank intermediaries, and can utilize them flexibly across global DeFi platforms for instant, low-cost transactions or diversified investments like tokenized real estate. This contrasts with bank fiat, where account restrictions, credit checks, and geographic limits curb user autonomy. Despite risks like smart contract vulnerabilities, DeFi's \$150 billion total value locked (TVL) in 2025 and \$27 trillion in stablecoin transactions in 2024 highlight its potential to redefine finance with efficiency and inclusivity.

Blockchain technology and cryptocurrencies are reshaping finance through decentralization, security, and innovation. By prioritizing stablecoin adoption over centralized central bank digital currencies (CBDCs), which risk replicating traditional vulnerabilities, policymakers can leverage blockchain's proven efficiency. With substantial growth year over year in stablecoin transactions

and growing institutional adoption (e.g., JPMorgan's Onyx platform processing \$1 billion daily), these technologies offer resilient alternatives to traditional systems. By fostering innovation-friendly regulations, the EU and U.S. can harness blockchain's potential, ensuring financial systems withstand economic shocks while driving digital progress.



One thing needs to keep in mind for future regulations who wish to let this innovative technology live out its potential - we cannot regulate our way into the future, but through balancing oversight and innovation, blockchain has the ability to redefine global finance.

Empowering European Businesses and Consumers Through Digital Payments

from Payments Europe's "True Value" study

The rise of digital payments is deeply shaping Europe's economic landscape. As cash usage declines, adopting digital payment methods fosters increased efficiency, security, and convenience for both consumers and merchants. In the latest report, Payments Europe surveyed over 13,000 consumers and 2,250 merchants across 13 European countries to assess the current state and future potential of the European payments market. The findings are compelling, highlighting how digital payments contribute to a more resilient and prosperous European economy, with key implications for businesses, consumers and overall economic growth.



The role of digital payments in Europe's future

The widespread shift to digital payments is driving substantial economic benefits for Europe. The study reveals that

72% of merchants now prefer digital payments over cash, 91% say that digital payments are critical for their organisation, and 85% report increased turnover from offering a wide range of payment options.

Digital payments streamline transactions, allowing businesses to operate more efficiently while reducing the operational costs associated with cash handling. This shift enhances cash flow management and empowers businesses to focus on growth and innovation.

Furthermore, the adoption of mobile wallets like Apple Pay and Google Pay is particularly strong among younger Europeans, further accelerating the shift towards digital. The study finds that 83% of consumers were relying on digital payments in the last 12 months, and 87% of consumers feel that the currently available payment options respond to their payment needs. This growing reliance on digital payments is fostering greater financial inclusion, allowing businesses of all sizes to reach a broader customer base and contributing to a more interconnected and resilient European economy.

The role of security and innovation in digital payments adoption

As digital payments become the norm, security remains a top priority for both consumers and merchants. The study highlights that 71% of consumers trust card payments more than any other payment method, while 46% of merchants consider cards the most secure method for preventing fraud. This trust in secure payment systems is essential for the continued growth of digital payments across Europe.

Ensuring transaction security is crucial not only for consumer confidence but also for economic stability. The rise of secure payment technologies like tokenisation and biometric authentication further enhances trust in digital systems, supporting their wider adoption. As consumers feel more confident in the safety of their transactions, their spending increases.

Innovation in the payments sector also plays a vital role in shaping Europe's economic resilience. The study reveals that 79% of merchants expect instant payments to grow in the coming year, and 61% of consumers support mandatory acceptance of digital payments. The increasing adoption of Buy Now Pay Later (BNPL) services and contactless payments is reshaping how Europeans pay and get paid, offering more convenient and flexible options. These innovations not only enhance the customer experience by providing faster, more accessible payment options but also enable businesses to expand their offerings, reduce transaction costs, and increase their reach.



Digital payments are vital to Europe's economic prosperity and resilience. By facilitating faster, more secure transactions, they enable businesses to grow, improve efficiency, drive innovation, and provide consumers with a seamless, secure, and convenient payment experience. As the digital payments sector continues to evolve, it will play an essential role in ensuring Europe's leadership in the global economy. Embracing this transformation will help strengthen Europe's economic future and foster a more inclusive, secure, and competitive financial environment.

Cybersecurity



Mastercard's commitment to cybersecurity

by Rigo Van den Broeck, Mastercard, Executive Vice President, Cybersecurity Solutions

The landscape of digital payments is transforming at an extraordinary rate. This evolution offers boundless opportunities for businesses and consumers alike, yet it also ushers in increased risks—fraud, scams, and cyberattacks loom ever larger.

Mirroring broader European trends, Slovenia is experiencing a sharp rise in payment fraud. With the rapid adoption of real-time and mobile payments, fraudsters are exploiting new vulnerabilities, prompting urgent responses from both the public and private sectors.

Financial scams surged by 22% over the past year and phishing accounted for 38%¹⁸ of reported incidents. Increasingly sophisticated threats are popping up on a global scale. Small and medium-sized enterprises are particularly vulnerable to ransomware attacks which have the potential to cripple their operations and compromise sensitive data.

The need for robust defenses is clear. Since 2018, Mastercard has invested over \$10.7 billion in cybersecurity innovation, creating industry-leading solutions designed to safeguard our customers while ensuring the security of the wider digital ecosystem.

Securing the payments ecosystem today must go beyond traditional defenses. Mastercard's multi-layered approach to cybersecurity encompasses four key pillars: prevent, identify, detect, and resolve. Each layer is reinforced with an array of advanced solutions that work in tandem to secure every stage of a transaction or interaction. Should one layer be breached, the next is activated immediately to halt the threat. Leveraging AI technology, Mastercard monitors over 19 million entities for cyber risks and vulnerabilities, stopping cyberattacks in mere seconds.

To address the growing threats of consumer fraud and cyberattacks, Mastercard has developed solutions such as TRACE (Transaction Risk Assessment and Control Engine), which uses real-time data to detect and prevent fraudulent activities before they can cause harm. This proactive approach ensures transactions remain safe and secure.

Moreover, the company has extended its reach in managing third-party risks through RiskRecon, which evaluates and monitors external vendors for vulnerabilities and offers continuous assessments.

Recognizing that threat intelligence is a cornerstone of modern cybersecurity, Mastercard's acquisition of Recorded Future has enhanced its capabilities in this domain. By integrating Recorded Future's cutting-edge threat intelligence services, customers can accurately identify emerging cyber threats and trends and swiftly respond to potential risks before they escalate.



¹⁸ <https://www.eesc.europa.eu/sites/default/files/files/ge-01-18-515-en-n.pdf>

While Mastercard continues to pioneer the use of advanced technologies and intelligence-driven solutions, and its global reach allows it to see trends that cross borders, we know that one organization cannot tackle cybersecurity risks alone.

In Slovenia, we work with partners including SICERT, the Faculty of Criminal Justice and Security, and specialized cyber security companies like Real Security, Viris and Go-Lix to identify and address threats.

Last year, Mastercard also established the European Cybersecurity Resilience Center, fostering collaboration among leading experts and partners to combat cybersecurity challenges collectively.

As the digital payments landscape continues to advance in Slovenia, Mastercard remains a steadfast partner in building a secure and resilient financial ecosystem. By harnessing cutting-edge technology, fostering collaboration, and prioritizing consumer protection, we can pave the way for a safer, more inclusive financial future for Slovenia and beyond.

Information Security as a Social Responsibility: The Need for Lifelong Awareness

by Blaž Markelj, University of Maribor, Associate Professor, PhD, Head of Chair

Trust in individuals and their work also means trust in the organizations they are part of. But this trust is not automatic—it depends on how responsibly we handle information: whether we know how to protect it, whether we understand its value, and whether we follow security guidelines.

In a world where access to data is fast and nearly unlimited, mobile devices and digital services have become key parts of our daily lives. However, this ubiquity of technology also introduces new vulnerabilities. Every device, every connection, and every user becomes a potential target for cyber threats. Especially in the era of remote work, these threats have intensified—attacks are increasing, methods are becoming more sophisticated, and the damage more severe.



Threats are no longer a thing of the future—they are part of our daily reality.

Ransomware, phishing emails, and misuse of personal data are no longer exceptions—they are a reality that demands action. But because these threats are often invisible and difficult for non-experts to understand, they are frequently overlooked or underestimated.

And this brings us to the key message: information security is no longer just a technical or organizational challenge. It is a social challenge. We need a knowledge base about the importance of information, threats, risks, and solutions—a base co-created by everyone: every ICT user, every organization, every decision-maker.

Security begins with people—starting with children.

If we want to ensure a high level of information security as a society, we must start early and remain consistent—from children, pupils, and students to employees, managers, and seniors. Everyone is a user of digital services, and therefore everyone must share the responsibility for security. This approach requires lifelong learning, which must be integrated into:

- **Formal education** (e.g., the University of Maribor's Faculty of Criminal Justice and Security, Information Security program),
- **Informal events**, such as the *Information Security Conference: Trust in People and Technology* (... , 2023, 2024, 2025),
- **Professional collaboration** established through the Competence Center for Cyber and Information Security at the University of Maribor's Faculty of Criminal Justice and Security.

In this way, we build a comprehensive system of knowledge transfer—academically, professionally, and socially.

Legislation provides the framework, but responsibility lies with the user and society.

With the new Information Security Act (ZInfV-1) and the EU NIS 2 Directive, Slovenia has laid a solid foundation for a well-regulated field of information security. The DORA Regulation further strengthens digital resilience in the financial sector. But legislation—no matter how precise—is not enough. Even the best security systems fail if a user doesn't recognize a phishing message, doesn't update their software, or doesn't follow basic security guidelines.

That's why it is crucial that each individual understands the technology they work with, the type of data they handle, and the value of that data. Without awareness, there is no protection.

Academia and practice—A two-way partnership

For years, the University of Maribor's Faculty of Criminal Justice and Security has been actively demonstrating that connecting education, research, and practice yields tangible results. Through study programs, research, and events (such as the annual *Information Security Conference*), the faculty educates future experts, raises awareness of the importance of information security, and fosters discussion on new challenges in cyberspace.

However, economic and public organizations also play a key role. They: Provide students with internships in real-world environments, Collaborate in developing solutions for real challenges, Help shape the competencies that the job market truly needs.

This creates a two-way flow of knowledge: academia provides expertise, while the business sector offers practice and direction. This connection is essential for developing a responsive and proactive workforce—one capable of tackling even the threats we do not yet know.

Conclusion: United for a Secure Digital Future

The future of information security is open and rapidly changing. But to be prepared, we must act together—academics, professionals, entrepreneurs, policymakers, and users. Security doesn't happen by itself. It is built through cooperation. That's why we need: Clear legislative foundations, Strong partnerships between universities and companies, and Above all, aware and responsible individuals of all generations.

Only then can we create a society where information security is a shared and self-evident value. Collaboration builds trust. And trust is the foundation of information security.

Security challenges and opportunities for banks

by Blaž Ozimek, Fraud Prevention & Management Coordinator, NLB d.d.

In today's hyper-connected financial ecosystem, security is no longer a back-office function, it is a board-level concern. The speed, complexity, and scope of threats facing banks have grown exponentially. From sophisticated cybercrime networks to socially engineered fraud targeting vulnerable customers, security risks are now systemic. For banks in smaller yet digitally ambitious markets like Slovenia, this global reality collides with local regulatory nuances and resource constraints.

The result: a dual challenge of keeping pace with global fraud trends while addressing local vulnerabilities within a strict compliance framework.



A Shifting Threat Landscape

Fraud is evolving at a pace that outperforms the adaptability of most financial institutions. While traditional typologies such as card-present fraud or first-party abuse remain relevant, they are rapidly being overshadowed by more sophisticated and elusive threats. These include authorized push payment (APP) fraud, synthetic identities, and increasingly, scams powered by generative AI.

At the heart of this transformation lies a new model: cybercrime is no longer the domain of isolated actors, but of highly organized, commercialized networks operating with the agility and scale of legitimate technology providers. This model, often referred to as Cybercrime-as-a-Service (CaaS)¹⁹, mirrors the structure of SaaS businesses, offering phishing kits, credential stuffing tools, ransomware payloads, and even money mule recruitment as packaged services on dark web marketplaces. Frequently delivered through subscription-based access, CaaS dramatically lowers the barrier to entry, enabling even non-technical individuals to launch complex and damaging attacks such as phishing campaigns, DDoS assaults, and extortion via ransomware²⁰.

Regulatory Complexity and Operational Pressure

Banks in the EU operate under a dense regulatory umbrella, PSD2 mandates strong customer authentication (SCA), GDPR demands data minimization, and national laws like Slovenian ZBan-3 and ZPPDFT-2 enforce stringent AML and operational risk controls. While well-intentioned, these overlapping rules often create friction in delivering seamless customer experiences and agile fraud prevention.

The paradox is clear: we are expected to block more fraud, faster, with less customer friction, while operating within rigid compliance boundaries. Additionally, local inter-agency cooperation (e.g., with SI-CERT or law enforcement) is often too slow or fragmented to respond to fast-moving fraud

¹⁹ Source: https://cybersecuritynews.com/cybercrime-as-a-service/?utm_source=chatgpt.com

²⁰ Source: https://dailysecurityreview.com/blog/cybercrime-as-a-service-caas-threat/?utm_source=chatgpt.com

waves. Law enforcement simply cannot match the speed of digital financial crime without structural change and real-time intelligence.

Legacy Systems, Fragmented Data, and Tactical Fatigue

Another pressing issue: many banks still rely on legacy fraud detection systems, which are rule-based engines designed for simpler attack vectors. These tools struggle in a world of dynamic, cross-channel fraud. Data silos between departments (payments, digital channels, customer support) further erode our ability to generate a single customer risk view or detect fraud patterns in real time.

Fraud prevention teams are increasingly stuck in reactive mode, as they are drowning in alerts, manual case reviews, and regulatory reporting. Rather than focusing on intelligence-led prevention or long-term strategy, they're trapped in a cycle of operational triage. This "tactical firefighting" may create the illusion of control, but it's unsustainable.

High false positive rates, alert fatigue, and customer friction erode both team efficiency and user trust. Analysts are consumed by repetitive tasks instead of focusing on high-impact threats. To break this cycle, banks must shift from fragmented, reactionary setups toward proactive fraud orchestration, integrating smarter analytics, streamlined processes, and cross-functional collaboration. Fraud teams should be empowered not just to detect, but to anticipate and influence strategic risk posture.

Opportunities to Transform

But there is hope and opportunity. Technology is no longer the constraint, mindset is. Banks must shift from fragmented point solutions to holistic fraud orchestration platforms integrating behavioural biometrics, device intelligence, machine learning models, and real-time transaction monitoring into a unified framework. Such systems allow for smarter decisioning with fewer false positives, and they scale without needing to hire dozens of analysts.

Customer education is also an underutilized pillar of security. Empowered customers can serve as the first line of defence. Campaigns that go beyond generic warnings using personalized, contextual nudges, that can significantly reduce fraud exposure.

Critically, we need better public-private partnerships. Banks, regulators, telecoms, and law enforcement must co-develop real-time threat intelligence sharing platforms. Estonia²¹ and the UK²² offer powerful examples, where fraud data is shared across sectors within seconds, not days.

Global Lessons, Local Adaptation

While the Slovenian market differs from larger ones, there is much we can adapt. The UK has pioneered reimbursement frameworks for APP fraud, forcing banks to prioritize prevention. The Nordics have shown how national identity systems (e.g., BankID) can drastically reduce fraud via

²¹ <https://e-estonia.com/solutions/interoperability-services/x-road/>


²² https://www.cifas.org.uk/fraud-prevention-community/external-threat-protect/national-fraud-database?utm_source=chatgpt.com

digital trust frameworks. In both cases, proactive regulation and sector-wide collaboration played key roles.

We must avoid copying these models blindly, but we can certainly localize best practices. Slovenia's compact banking ecosystem is an advantage that allows for faster coordination, clearer governance, and the potential to leapfrog outdated models.

Conclusion

Security is no longer just about compliance – it's about resilience. It's about building systems, processes, and cultures that assume breaches will happen, but are designed to detect, contain, and recover quickly. Fraud prevention must evolve from a reactive compliance cost centre to a proactive, intelligence-driven capability embedded in product design, customer journey, and strategic planning. The time to invest is now. Because in the battle for trust, those who move first, and move smart, will define the next chapter of secure banking.



True resilience starts
when we stop reacting
and start outsmarting.

TTP Framework: A Structured Approach to Understanding and Countering Cyber Threats

from Mastercard's "The Age of Cybercrime" report

Effective cybersecurity begins with understanding how malicious actors think, plan, and operate. One of the most effective tools for analysing and anticipating attacker behaviour is the TTP framework, which breaks down attacks into three fundamental components: Tactics, Techniques, and Procedures. This structure enables defenders to interpret the logic of an attack and craft precise, targeted responses at each level.



1. What Is the TTP Framework?

The TTP model helps decode the anatomy of a cyberattack by categorizing it into:

- **Tactics** – the high-level strategic goals of the attacker (e.g. stealing data, causing disruption). These tend to change slowly, as they reflect broader intent rather than specific methods.
- **Techniques** – the general methods used to achieve the tactics, such as phishing or exploiting a software vulnerability. These evolve moderately as new tools and methods emerge.
- **Procedures** – the detailed, context-specific actions attackers take to implement the techniques. These are highly dynamic and responsive to external events, such as media coverage, global crises, or software failures.

To demonstrate how this works in a non-technical setting: A car thief wants to steal a luxury vehicle (tactic). Instead of breaking in, they decide to impersonate a valet attendant (technique). They wear a fake uniform, confidently approach the car owner, and use polite language to gain trust (procedure).

Cybercriminals operate in a strikingly similar manner—only in digital environments.

2. How the TTP Framework Helps Us Understand Attacker Agility

The rate of change across the three layers of TTP is uneven—and this has significant implications for defense:

- Tactics remain relatively static. These can be addressed through long-term education, AI-based pattern recognition, and strategic technology investments.
- Techniques change more slowly and can be countered by maintaining a strong security posture, including regular vulnerability assessments and platform-level resilience.
- Procedures, however, are constantly evolving, especially in response to high-profile events. These require real-time situational awareness and rapid communication to end-users.

A clear illustration of attackers' adaptability is the CrowdStrike incident in July 2024, when a faulty software update caused widespread outages impacting critical sectors such as healthcare, aviation, and emergency services. Within a day, cybercriminals capitalized on the disruption by launching phishing campaigns and fake support sites that offered fraudulent "hotfixes," which in

reality installed malware like HijackLoader. This was not a new method or tactic, but rather an adaptation in their procedures, designed to exploit the confusion and urgency.

A comparable case occurred in mid-2025 following significant tariff announcements by U.S. President Donald Trump during his current term. As media coverage intensified around rising import duties—especially on consumer electronics and vehicles—threat actors swiftly took advantage. Within days, fraudulent websites and targeted social media ads surfaced, promoting fake “tariff compensation” or “early refund” initiatives. These schemes promised substantial payouts, enticing victims to disclose sensitive personal and financial information under the pretence of official verification. Many attackers employed generative AI technologies to craft highly realistic websites mimicking legitimate government portals. Once again, this was not a fundamental change in tactics or techniques, but a rapid procedural adjustment aligned with an emotionally charged political event.

Together, these examples underscore the critical advantage held by contemporary attackers: their speed and responsiveness. Their capacity to monitor global events, pinpoint societal vulnerabilities—whether technical or psychological—and quickly develop customized attack scenarios enables them to stay ahead of conventional defenses. Consequently, effective cybersecurity requires defenders to look beyond static tactics and techniques, emphasizing continuous vigilance and adaptability to swift procedural evolutions driven by changing social, political, and economic dynamics.

3. TTP as a Defensive Framework

The value of the TTP model lies not only in its explanatory power, but in its ability to guide strategic defense. By breaking down threats into their core components, we can avoid generic solutions and instead deploy the right tools at the right level.

TTP Layer	Individuals	Businesses
Procedures	Situational awareness, scepticism toward unsolicited contact	Thoughtful UI/UX, responsive support mechanisms
Techniques	Reflex-level security habits (e.g. password hygiene)	Continuous monitoring, patch management, security audits
Tactics	Foundational education, media literacy	Long-term innovation, AI-based threat modelling

Traditionally, cybersecurity has treated infrastructure protection and end-user awareness as separate domains. However, as attackers increasingly exploit the human factor (e.g. social engineering, manipulated trust), these silos must break down. No single solution—be it user education or backend security—is sufficient on its own.

Instead, resilience emerges when we identify the right type of response for each component of the threat. The TTP framework provides this clarity, enabling defenders to think modularly, act strategically, and keep pace with an adversary that thrives on unpredictability.

Regulation



Open Strategic Autonomy: international collaboration, sound regulatory oversight and innovative legal frameworks

By Mikael Svensson, Mastercard, VP, Government Affairs Europe

Sparked by increased geopolitical tension, the EU has progressively striven towards greater strategic autonomy and resilience with the aim of reducing dependencies on other countries and foreign providers. Strategic autonomy has become one of the European Commission's most important policy guidelines in recent years, with Member States committing to this for the long term with the Resilient EU2030 programme. It is expected that increasing autonomy and strengthening the EU's position as a global player will remain highly relevant for the next European Commission mandate.



Mastercard is convinced that promoting open strategic autonomy through international collaboration and public-private partnerships, while ensuring sound regulatory oversight and innovative legal frameworks, can form the basis for Europe's prosperity.

We fully support and understand the need for greater resilience and autonomy. In fact, we firmly commit to Europe and its values and have supported European businesses and citizens through our expertise and offering in payments and beyond for over 50 years. However, we emphasise that resilience should not be simply interpreted as locally designed as like-minded global companies bring much value to Europeans and are crucial for supporting the robustness of the European Single Market whilst strengthening the security of the Digital Economy. To exemplify this, the international card schemes support the Strong Customer Authentication (SCA) system, which is mandatory for accessing payment accounts online and initiating an electronic payment transaction under the Second Payment Services Directive (PSD2). Moreover, Mastercard enhance Open Banking by facilitating connectivity between Third-Party Payment Service Providers (TPP) and Payment Service Providers (PSP) and support the European PSPs with products like click-to-pay, formulating a competitive response against the BigTech companies moving into the European payment market. This is vital as the entrance of BigTech to the European payments market carries risks, e.g., market dominance, privacy issues, and algorithmic discrimination.

Supply chain management is key to improving Europe's resilience

Global trade and economy are keys to wealth worldwide, and innovation occurs globally. For Europe's resilience and open strategic autonomy, it is essential to remain open for international companies committing to European values and the common goal of driving Europe's economy forward. It is crucial for the EU to maintain its competitiveness while managing mutual dependencies and increasing the level of autonomy at the same time. As there is no positive correlation between the geographic proximity of a company's origins and its safety and/or resilience, selecting European-born support structures by default would risk technological fragmentation and be counterproductive to Europe's ambitions to decrease dependencies and

increase its economic power. Instead, the EU should focus on nurturing global supply chains whilst optimising their resilience by detecting, among others, geopolitical and cyber risks and making educated, evidence-based decisions. Such collaboration enables the EU to protect European businesses and citizens from potential external risk factors and determine the best course of action in the evolving geopolitical context and rapid digital shift. Companies can play a pivotal role in detecting and mitigating potential risks to supply chains through data. However, to ensure a high level of security for all European supply chains, it is pivotal for the EU to collaborate with the industries to create a legislative framework and standards to prevent fragmentation within the EU market. For instance, cybercrime is a major threat to any industry and is not bound by geographical borders. Thus, the most efficient responses to cybercrime are often global, and companies with global reach, hence, with access to global cybercrime data, significantly contribute to the security of the Digital Economy.

Initiatives such as the digital euro, designed to strengthen the euro's international role and introduce a digital European currency to complement cash, will only succeed in reaching their full potential if the best suitable technologies are harnessed for their support and distribution. Hence, to remain globally competitive, the technologies supporting Europe's open strategic autonomy should not be limited to European-born solutions if better international alternatives are available, as this would likely result in a disadvantage in the global market. Furthermore, the private sector's contribution to supporting initiatives such as the digital euro can be vital for their success, as their practical expertise and solutions often have a major role in creating a convenient and effortless customer journey for the users, which in turn bolsters the uptake of innovative services. Therefore, we encourage the EU to establish further public-private partnerships (PPPs) to support greater open strategic autonomy and resilience of the European economy.

Updating the oversight framework

The European payments ecosystem is highly vibrant – never in history has a generation of EU citizens had more options and choices of digital payments (3-party, 4-party, and domestic card schemes, Buy-Now-Pay-Later, invoice, cash on delivery, instant payments, etc.), and new payment methods, e.g., crypto, tokenisation and Central Bank Digital Currencies (CBDCs) are entering the market. The rapidly evolving digitalisation and global connectedness have resulted in increasing complexity of the markets and technologies. To foster a secure, innovative, inclusive, and convenient digital economy, the oversight framework must be fit to facilitate new technologies, lift barriers to cross-border operations, incentivise interoperable and integrated services. We applaud the EU for taking steps in the right direction, such as the proposal for a framework for financial data access (FIDA), as ultimately, developing clear rules prioritising strong consumer protections, stability, and regulatory compliance whilst avoiding unnecessary legislative complexity is essential for enabling secure and more efficient payment and commerce applications through such technologies. Furthermore, ensuring harmonisation between horizontal and vertical regulation should be prioritised, e.g., the interplay of the PSD2 and GDPR has not been seamless, ultimately requiring the European Data Protection Board to update the related guidelines. With this in mind, for the EU to be successful in increasing Europe's competitiveness, it is essential that the rules, e.g., SCA and Open Banking, etc., are applied in the same way across the member states, as this will enable businesses, including SMEs, to scale up and grow. Therefore, it is vital that the competent

authorities are equipped with the resources and capacity to fully understand the markets and technologies. Furthermore, as the payments market develops, it is important to update the existing oversight framework, e.g., SIPS, PISA, and DORA.

While developing rules and standards for tomorrow's payments, it is vital to work closely with the industry, holding practical experience and expertise as well as data on innovative solutions, to address these innovations promptly and make the most effective decisions to support innovation whilst managing potential risks. Thus, we encourage the EU to embrace the benefits of PPPs.

The EU must remain a global standard-setter

It is vital to strengthen international cooperation and consensus on digital governance issues to foster a secure, innovative, inclusive, and convenient digital economy.

We are convinced that the EU should continue setting future-proofed interoperable and open security standards and liaising with international partners to make them global, as successfully established in several aspects, such as the processing of personal data under the GDPR.

We believe that optimising the security of global supply chains and establishing international standards for them is in the interest of the functioning of these value chains and can foster the participation of all business types and sizes, as fractioned standards and legislation between jurisdictions require an additional investment of funds and resources from the companies to comply with the different rules applied for the same action. In this regard, industries and global companies can also play a pivotal role in applying the EU-born standards globally, thus streamlining them across the globe and fostering a level playfield in Europe and beyond. Therefore, working closely together with the industries can support the global application of the European market rules and standards. To exemplify, Mastercard has made the GDPR, as well as encouraged streamlining best practices for products and services in the EU market, a global standard in conducting business.

Strengthening Economic Resilience through a Competitive Taxation System

by AmCham Slovenia, Finance Committee

In the current global environment, where economic dynamics are rapidly evolving, Slovenia must urgently reassess the competitiveness of its taxation system. In the latest IMD World Competitiveness Ranking for 2024, Slovenia ranked 46th out of 67 economies—an unchanged position compared to the previous year and a sign of stagnation amid increasing global competition. This reflects concerns about tax policy, regulatory burden, and labor market flexibility, all of which require urgent reform. A well-designed, transparent, and growth-oriented tax system is not only

vital for attracting investment and talent, but also for ensuring economic resilience in the face of external shocks. As highlighted by the IMD Competitiveness Ranking, Slovenia has shown stagnation in its positioning, which clearly signals the need for systemic reform. Without a decisive shift, the risk of further decline in competitiveness—and in turn, economic stability—will only increase.



A competitive taxation system fosters economic growth by incentivizing productivity, innovation, and investment. It reduces the burden on businesses and individuals, thereby increasing disposable income, enabling reinvestment, and encouraging entrepreneurial activity. For Slovenia, this means undertaking comprehensive reforms to simplify and modernize the current tax framework, with a strong focus on predictability, fairness, and efficiency. An effective tax strategy can create the foundation for a more dynamic and opportunity-rich economy, which benefits both the private and public sectors.

Financial and economic stakeholders in Slovenia agree that the current tax burden—especially on labor and high-skilled professionals—is counterproductive. High personal income taxation disincentivizes productivity and the retention of top talent, while rigid corporate tax rules often hinder reinvestment and expansion. A reduction in tax wedges and a more progressive shift toward consumption-based taxation could support long-term economic sustainability and align Slovenia with best practices seen in more competitive economies.

Additionally, tax reform must not occur in isolation. Our Finance Committee emphasizes that taxation is one of several pillars supporting competitiveness. For instance, a tax system that does not align with efficient judicial processes or timely public procurement hinders implementation and investor confidence. Moreover, strong education and healthcare systems, funded by effective tax collection and allocation, directly affect workforce quality and productivity—critical factors in long-term economic performance. Effective reforms must therefore be complemented by improvements in regulatory agility, a faster and more efficient judicial system, and consistent investments in research, development, and infrastructure. These dimensions are deeply interlinked and mutually reinforcing.

AmCham Finance Committee and our business community advocate for:

1. **Lowering the tax burden on labor:** Gradually reduce personal income tax rates, especially in the middle and upper-middle brackets, to enhance net wages and reduce brain drain. A more balanced tax mix would support labor market activation, particularly among young professionals.
2. **Stability and predictability:** Establish long-term fiscal policies with minimal annual fluctuations to foster a stable environment for foreign and domestic investors. Frequent tax changes increase administrative burdens and reduce trust in the system.
3. **Modernizing tax administration:** Invest in digital tax tools, risk-based audits, and simplified reporting procedures to reduce compliance costs and increase transparency. Better integration of data systems can support both taxpayers and tax authorities in optimizing efficiency.
4. **Encouraging innovation and green transition:** Introduce targeted tax credits for R&D, digitalization, and sustainable transformation. Special incentives for companies investing in climate-friendly solutions and knowledge-based sectors can serve as a key driver for long-term growth.
5. **Shifting towards efficiency-based taxation:** Increase the share of indirect taxes (e.g., VAT), while ensuring proper compensation mechanisms for vulnerable groups. This could ease pressure on productive income and reward reinvestment.
6. **Addressing the grey economy:** Strengthen tax enforcement through data-driven oversight and inter-agency cooperation. Reducing informality will broaden the tax base without raising rates.
7. **Fostering public-private dialogue:** Ensure inclusive policymaking by involving key economic stakeholders early in the legislative process. Transparency and consistency in tax policy are essential for building investor confidence.

A competitive tax system not only enhances economic output but also strengthens resilience. Resilient economies are better equipped to manage inflationary pressures, geopolitical tensions, and technological disruption. Tax competitiveness attracts long-term investors, boosts employment, and reinforces the overall social fabric through better public service funding. It also ensures that economic recovery is broad-based and sustainable.

In conclusion, we must view tax reform not as a standalone goal but as an essential pillar in the broader strategy for national competitiveness. It requires political courage, cross-sector collaboration, and a clear long-term vision. Slovenia stands at a crossroads: with bold and well-structured reforms, it can move decisively up the global competitiveness ladder. If action is delayed, the cost of inaction may far exceed the effort required for change.

--

Prepared with consideration of the perspectives of the AmCham Finance Committee and aligned with the principles outlined by the Economic Circle²³.

²³ Economic Circle – Gospodarski krog is a group of chambers, business associations, agricultural organizations and combines 17 different stakeholders.

Regulatory considerations for the improvement of the Slovenian banking sector

by Stanislava Zadavec C., Director, The Bank Association of Slovenia

Introduction

The banking sector plays an important role in the stability and development of economies. It facilitates financial intermediation, ensures liquidity, and supports investment. However, because banks are deeply interconnected with the economy, their failures can trigger widespread losses far beyond shareholders. In this sense, bank regulation and supervision are essential: they safeguard stability by ensuring banks holding adequate capital, liquidity, and risk controls.

Following the 2008 global financial crisis, regulatory reform intensified worldwide. The crisis exposed critical weaknesses in supervision and risk management. Consequently, international frameworks like Basel III were introduced to enhance the resilience of banks through stricter capital requirements, leverage controls, and enhanced supervision. Empirical evidence shows that the post-2008 framework has indeed built resilience.

Recently regulatory architecture has further evolved, integrating environmental, social, and governance (ESG) considerations into banking system. The European Green Deal and the Sustainable Finance Disclosure Regulation (SFDR) mandate transparency on sustainability risks. Simultaneously, digital transformation and the proliferation of fintech have prompted the adoption of regulations designed to mitigate cyber threats and IT disruptions.

In the last decade the European Union (EU) has been operating under a harmonized yet complex regulatory framework. The Single Supervisory Mechanism (SSM) and the Single Resolution Mechanism (SRM), both under the umbrella of the Banking Union, aim at ensuring uniform standards across member states. Yet, despite these reforms, EU banks lag compared to their international peers in profitability and global market share. A key reason is structural: the EU's Single Market is still incomplete, so banks face twenty-seven seats of national rules. By contrast, US banks operate under one federal regime, allowing larger institutions to scale nationally. Thus, regulatory fragmentation in the EU – across prudential, accounting, insolvency and other laws raises business costs.

This is one of the reasons explaining the competitiveness gap observed by comparing the profitability of banking sectors at the global level. The industry data shows that US bank returns on equity have consistently outpaced those of European peers in last decade and, according to The Banker report, "US banks have surged ahead with 17% profit growth in 2024, widening the gap with struggling European and Chinese lenders"²⁴



²⁴ Thebanker.com

While currently Europe still ranks second on the TAB Global 1000 (top 1000 banks), which together held about \$160 trillion in assets (Asia-Pacific: 48.8 %, Europe: 28.7 %, North America (mainly U.S.): 17.4 %), McKinsey's broad asset growth figures indicate that from 2015–2022 North America's banking assets rose by ~\$13.3 trillion, Europe's banking assets rose by ~\$4.2 trillion; Asia (excluding China) added ~\$11.2 trillion and; China alone added ~\$22.7 trillion.²⁵

The EU banking sector seems to lag global competitors also in digital adoption. Asian banking systems are known for mobile-first ecosystems (Alipay, WeChat Pay in China; Paytm and UPI in India) and high fintech integration resulting in strong occurrence of digital – only banks. United States are known for their innovation hubs, leading in tech-finance collaborations (Apple Card, Google Wallet, Amazon Pay...) and strong cloud banking. Meanwhile the EU is known for its regulatory leadership (PSD2 open banking, GDPR data governance, eIDAS digital identity frameworks, DORA digital operation resilience) and heavy focus of traditional banks on compliance which comes at cost of innovation lag as result of lesser agility. At the same time different types of non-bank lenders in Europe (and globally) have grown significantly.

Historical economic cycles as well as recent experience show that resilience fosters reliability and capacity to finance but, the current global environment, marked by financial instability, technological change, and environmental urgency, demands that regulators adopt agile, forward-looking, and cooperative approaches to enhance competitiveness of the economies. Across global regions, there is broad agreement that regulatory frameworks must stay robust enough to ensure safety, but at the same time simple enough to allow banks to compete and innovate.

Rebalancing Robustness and Simplification

The current US administration has signaled a deregulatory turn, and the European Parliament likewise has urged simplification of capital and loss-absorbency rules but insists that any changes shall not weaken aggregate requirements²⁶. The ECB emphasizes "simplification without deregulation" and its agenda includes refining supervisory processes (SREP) and promoting one-stop shop rules, while preserving high capital and liquidity standards. As ECB SSM Chair Mrs. Buch puts it, regulators must ensure efficiency "without sacrificing resilience"²⁷. In practice, this means eliminating redundant reporting and harmonizing definitions (e.g., standardizing how risk-weighted assets are calculated across banks) so that banks spend less on compliance and more on core activities.

Banking industry for some time already stress simplification

The European banking sector through European Banking Federation (EBF) already for some time jointly argues that regulatory complexity is undermining the EU's competitiveness and calls for clear and proportionate regulation to unlock lending for the green and digital transitions.

It highlights burdens of tax, reporting and even sustainability rules, and urge policymakers to streamline them.

²⁵ EBA, McKinsey & Company

²⁶ [Europarl.europa.eu](https://europarl.europa.eu)

²⁷ [Ecb.europa.eu](https://ecb.europa.eu)

The complexity and volume of financial regulation at the European level, has resulted in a dense, bureaucratic and often unstable regulatory environment. To address the challenges of the major contributing factors underlying lesser competitiveness of the EU banking system, the EBF, together with the European Association of Co-operative Banks (EACB), the European Savings and Retail Banking Group (ESBG) and an ad hoc group of European law professors, lawyers and banking law experts, co-authored the “Less is More” report (the Report) ²⁸. The Report in summary proposes the following areas of actions aimed at simplifying the EU banking regulatory framework while preserving overall resilience and supervisory strength:

Focus Area	Simply Competitive Proposal Highlights
Strategic Recognition	Declare banking sector strategic - aligning regulation around competitiveness
Capital Requirements	Reconsider EU-specific capital overlays; simplify MREL/TLAC; revive securitization
Framework Simplification	Cut rule fragmentation, harmonize national discretions, reduce reporting noise
Capital Markets Strategy	Complete CMU, simplify retail investment access, enable securitization
Digital & Data Policy	Flexibly design digital euro/FiDA, assess competitive impacts before roll-out
Supervisory Philosophy	Shift toward enabling growth and innovation - not excessive conservatism

Ultimately, the guiding principle is that resilience and competitiveness can be complementary, not contradictory. The Report proposes a pragmatic and balanced simplification of the EU banking regulatory framework. The goal is greater clarity, reduced compliance costs, and improved competitiveness while maintaining robustness and regulatory integrity.

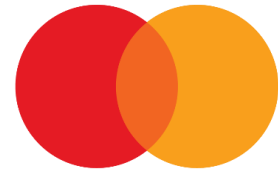
The practical recommendations span rule rationalization, reporting harmonization, calibrated capital requirements, and governance reforms to make EU regulation both effective and efficient.

²⁸ Ebf.eu

Roadmap towards a resilient, prosperous, and liveable Europe

from Mastercard's "Manifesto on the Future of Europe"

With Europe being at the beginning of its next legislative cycle, we at Mastercard have a clear vision to address the main challenges ahead of us. We suggest 14 recommendations that aim to contribute to building a resilient, prosperous, and liveable Europe while tapping into the full potential of innovative technologies – ultimately improving the lives of European citizens.



Our recommendations refer to four key policy priorities:

- (1) Open Strategic Autonomy
- (2) Vibrant Digital European Economy
- (3) Innovation Leadership
- (4) Liveable Future

(1) Fostering Open Strategic Autonomy through international collaboration, sound regulatory oversight and innovative legal frameworks.

We are convinced that promoting open strategic autonomy through international collaboration and public-private partnerships, while ensuring sound regulatory oversight and innovative legal frameworks, will form the basis for Europe's future success.

1. A key component of open strategic autonomy is best-in-class regulatory oversight, across sectors. Maintaining and, where necessary, adapting existing supervisory regimes should be a key priority.
2. To avoid digital fragmentation, we encourage the EU to collaborate with the international community to establish globally interoperable and open standards, including fostering public-private partnerships.
3. We urge the EU to remain a standard-setter for innovative regulation of the digital economy, especially lifting barriers to cross-border services within the EU, enhancing integrated and interoperable services.

(2) Creating a Vibrant Digital European Economy by enabling businesses and citizens to thrive and master cybersecurity and fraud challenges, while further extending targeted support programs.

As a cybersecurity leader, we believe that businesses and citizens must be equipped with the skills and tools to thrive in the digital economy and be able to deal with the increasing challenges of cybersecurity and fraud detection. Combined with targeted support programs, aimed at accelerating the digital transformation, the EU will unlock its full economic potential.

4. We call on the EU to focus on lifting barriers to the cross-border provision of services and supporting companies, especially SMEs, in their transition to a digital economy, for example by updating the SME Strategy and the 2020 Digital Finance Action Plan.
5. We ask the EU to implement and further develop the 2023 European Skills Agenda, incentivising private sector engagement, to bridge the digital divide and improve digital literacy of all citizens.
6. We encourage the EU to work together with the private sector to launch initiatives to combat cybercrime and to prepare fallback mechanisms to address those risks.
7. We recommend that EU policies enable and facilitate the use of emerging technologies, such as AI and biometrics, to strengthen the fight against fraud and financial crime to create a safer and more secured environment for citizens and the industry.

(3) Ensuring responsible Innovation Leadership by tapping into the full potential of new technologies, while creating trust in them.

We are certain that a prosperous Europe can only be achieved through a clear focus on innovation leadership in key industries. To this end, the potential of new technologies, including AI and the use of data, must be fully and responsibly exploited while building trust in them.

8. We call on the EU to safeguard an environment that promotes and facilitates secure and trusted cross-border data flows, focused on the protection of fundamental rights of citizens and legal certainty for businesses.
9. We also support EU's efforts in further encouraging data sharing and the creation of data ecosystems helping to unlock innovation in all markets to the benefits of the EU's economy and society at large.
10. We urge the EU to prepare a communication for fostering e-government services as well as encouraging digitalization of public finance management for higher public services efficiency and inclusion for citizens.
11. We encourage the EU to generate a strategy fostering a secure and innovative environment for virtual worlds and extended realities.

(4) Securing a Liveable Future through creating tools, frameworks and initiatives across industries that enable businesses and citizens to fully commit to sustainability.

We urge the EU to further accelerate sustainability efforts through enforcing the necessary laws whilst creating tools and initiatives across industries to enable businesses and citizens to fully commit to sustainability.

12. We urge the EU to set ambitious implementation timelines and strong enforcement for legislation such as the Digital Product Passports and the Carbon Removal Framework.
 13. We are convinced that smart cities should become the norm. Therefore, we ask the EU to take steps aimed at harmonising and simplifying urban mobility, such as facilitating the acceptance of universal digital payments easing consumer access to sustainable means of transportations across Europe.
 14. We encourage the EU to launch a strategy that supports the transition towards a more sustainable, resilient and inclusive tourism economy.
- 

