Securing Internet Payments across Europe

Guidelines for Detecting and Preventing Fraud

VASCO
THE AUTHENTICATION COMPANY

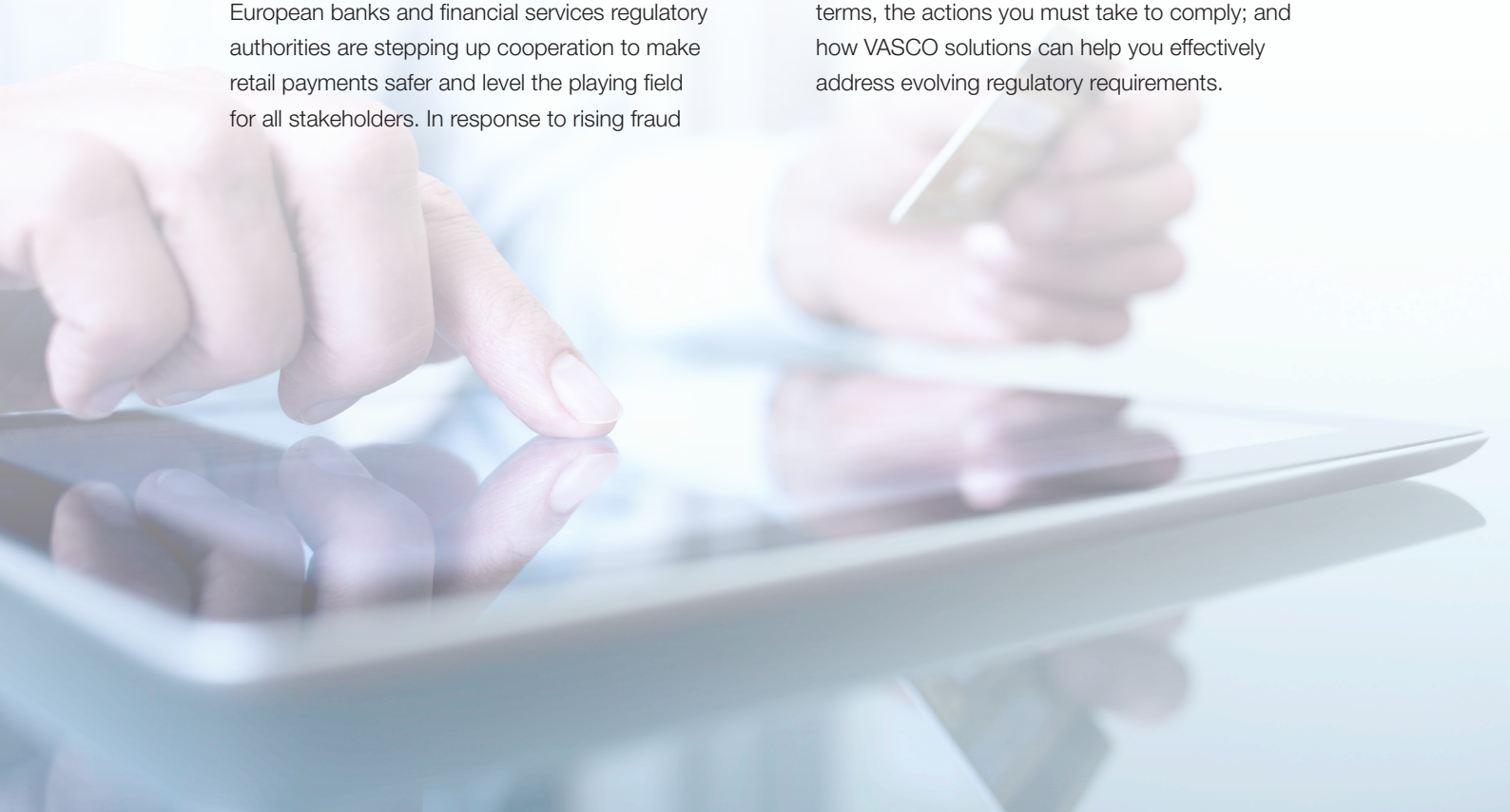
Table of Contents

Executive Summary

Increasingly frequent and highly sophisticated cyber-attacks continue to permeate every pathway that crosses the digital landscape. The multiple online channels financial institutions and other payment service providers (PSPs) use to facilitate e-banking and e-commerce are irresistible targets for fraudsters. Evolving security threats and advanced technologies are subjecting internet commerce to significantly higher rates of fraud than traditional payment methods. Banks and other service providers face an urgent need to deploy more powerful mechanisms to detect and prevent fraud within the internet payments domain. They must enhance their risk analysis and authentication capabilities. A simple authentication server, basic data mining, and back-office decision analysis are no longer proactive or sufficient enough to manage the complexity or sophistication of today's fraud. The pace and intricacy of cybercrime in the electronic payment environment demand an agile and savvy defence.

European banks and financial services regulatory authorities are stepping up cooperation to make retail payments safer and level the playing field for all stakeholders. In response to rising fraud levels and consumer security concerns, the European Central Bank (ECB) published detailed recommendations for the security of internet payment operations in an effort to identify major vulnerabilities, nurture a common knowledge and understanding of inherent risks among European Union (EU) Member States, and establish a foundation for consistent regulatory oversight of payment services, systems and schemes. EU nations are encouraged to adopt these recommendations and best practices in order to collectively fight online payment fraud, enhance customer trust, and harmonize internet payment security across Europe.

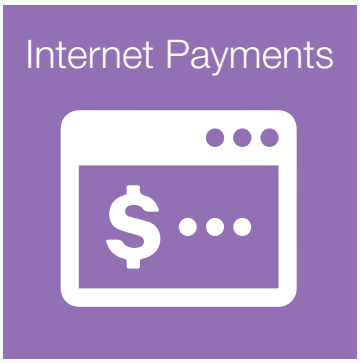
In this paper, VASCO, a leading provider of internet security solutions, delivers tangible guidance on compliance. We highlight critical elements of the recommendations impacting participants in the internet payment services ecosystem—specifically global, national and regional banks; credit card companies; and other payment service providers. We tell you what you need to know; explain, in practical terms, the actions you must take to comply; and how VASCO solutions can help you effectively address evolving regulatory requirements.



Protecting Internet Payments: A Top Priority for All Stakeholders

Internet payment solutions offer consumers a more convenient way to purchase goods and services online. However, these digital transactions represent a major attack vector for cybercriminals. Security issues remain a significant concern for both service providers and their customers. Banks and PSPs must deploy more effective security mechanisms in order to safeguard their assets and improve consumer protection and confidence. Early fraud detection and prevention translate into lower costs, less customer impact and reduced regulatory scrutiny.

The European Central Bank Recommendations for the Security of Internet Payments are organized into two categories of control and security guidelines. The first set of general recommendations for controlling the security environment focuses on governance and risk management procedures. The second group of guidelines drills down into specific control and security measures for online payments, including strong customer authentication, delivery of authentication tools, access controls, transaction monitoring, and sensitive payment data protection.



"28% of users are not confident about using the internet for banking or shopping."

Special Eurobarometer 404 – Cyber Security (European Commission)

The ECB recommendations are based on four guiding principles that all participants in the internet payment services business are encouraged to adopt and implement:

- Monitor and periodically assess relevant risks associated with providing internet payment services.
- Protect initiation of payments and access to sensitive data with strong customer authentication.
- Proactively monitor transactions to enable identification of abnormal payment patterns.
- Educate customers to enhance their awareness and understanding of internet payment security.

The following six ECB recommendations are top priority for financial institutions, PSPs, and all other players in the internet payment services market. Adherence to these guidelines will facilitate compliance with evolving regulatory requirements as they are translated into law EU during the next two years (see sidebar: European Regulatory Initiatives for Securing Internet Payments). Banks and PSPs are responsible for implementing technologies and practices that enable mitigation of assessed risk. VASCO helps financial institutions and PSPs secure their online channels. Below each key recommendation is a snapshot of how VASCO's IDENTIKEY Risk Manager solution can help banks and PSPs achieve compliance.

IDENTIKEY Risk Manager: Comprehensive Fraud Protection

IDENTIKEY Risk Manager is a server-side risk management platform that adds an innovative layer of intelligence to authentication management, enabling payment service providers to proactively and rapidly detect and prevent fraud across multiple channels. IDENTIKEY Risk Manager:

- Dynamically monitors, analyses and reduces volume of fraudulent transactions
- Accelerates response to fraud patterns and new threats
- Creates barriers hackers and fraudsters cannot easily circumvent
- Invisibly keeps users and transactions secure without requiring unnecessary authentication
- Enhances security without sacrificing user convenience and efficiency
- Minimises impact on daily workflows and facilitates adoption of fraud prevention measures
- Simplifies and streamlines compliance with evolving regulations

European Central Bank Control and Security Recommendation Priorities

Transaction Monitoring

All participants in the internet payment services ecosystem should employ fraud monitoring mechanisms to detect and prevent suspicious or high-risk transactions prior to authorization. This includes tracking abnormal customer behaviour and access device patterns, monitoring e-merchant activities, and identifying known fraud scenarios.

- Monitors transactions across multiple channels, challenges unusual and suspicious patterns and behaviours, and initiates protective action on demand
- Detects fraudulent activities, enabling quick response to evolving fraud patterns in threat landscape
- Reduces PSP chargeback costs associated with refunding money to consumers
- Decreases number of suspicious transactions security teams must mitigate, thereby lowering operational costs and resource requirements
- Facilitates fast and frictionless payment experience across channels

Verify Transactions with VASCO IDENTIKEY Risk Manager

Strong Customer Authentication

All internet payments and access to sensitive payment data should be protected by strong customer authentication. This applies to all online payment market participants, instruments and transactions, including e-merchants, banks, credit card and virtual card issuers and holders, wallet solutions, transfers, debits, and access to customer information that could be used to commit fraud. ECB recommends that PSPs consider using one strong customer authentication solution for all internet payment services to increase acceptance and facilitate proper use among customers.

Simplify Authentication with VASCO IDENTIKEY Risk Manager

- Uses risk-based authentication technology to evaluate profiles of users requesting access and determines risk associated with the transactions
- Relies on additional credentials and contextual information (i.e., user location, device characteristics, transaction amount) when presented with high-risk profiles
- Applies appropriate level of authentication to ease process when less security is required and steps up to more stringent methods when potential fraud is detected

Risk Control and Mitigation

Implement multiple layers of defence to mitigate identified risks. All internet payment services should be built on a foundation of sound identity and access management. Ensure robust security solutions are in place to protect networks, websites, servers and applications from attack. Monitor and restrict access to sensitive payment data and critical resources.

Protect Assets with VASCO IDENTIKEY Risk Manager

- Gathers behavioural, contextual, qualitative and quantitative data
- Harnesses data and converts it into actionable intelligence for real-time fraud detection and prevention
- Taps into the power of sophisticated risk analytics to dynamically predict, identify, assess and score risks
- Reduces fraudulent activities across channels via integrated analytics and intelligence

Monitoring and Reporting

Banks and PSPs should have a process in place for consistently monitoring and reporting on security vulnerabilities in payment systems. In the case of significant breaches related to payment services, notify appropriate oversight authorities and law enforcement agencies. Require all payment services partners (i.e., e-merchants) to cooperate.

Track AML Activity with VASCO IDENTIKEY Risk Manager

- Continuously monitors transactions to identify, track and report suspicious activity related to Anti-Money Laundering (AML)
- Analyses and integrates data from multiple channels (electronic payments via online and mobile banking instruments including credit and debit cards, direct debits, wire/credit transfers, prepaid cards and vouchers, e-checks, e-wallets)
- Features comprehensive and customizable self-service reporting tools that reduce demands on internal staff

Customer Identification and Information

Customers should be properly identified per European Anti-Money Laundering legislation before being granted access to internet payment services. Also, PSPs must clearly communicate all mandatory procedures and requirements related to proper and secure use of internet payment service equipment, technology and user credentials.

Secure Access with VASCO IDENTIKEY Risk Manager

- Rapidly detects and prevents improper access and account takeover through tracking, identification and analysis of user personas, devices and applications across channels
- Identifies suspicious login patterns, tracking access attempts from high-risk or compromised devices and users
- Requires additional authentication before granting access to potentially malicious users
- Monitors and assesses risk associated with all user profile and beneficiary changes

Governance

Implement and regularly review a formal security policy for internet payment services. The policy should encompass security objectives, risk appetite, sensitive data management, and defined roles and responsibilities.

Ensure Compliance with VASCO IDENTIKEY Risk Manager

- Integrates flexible policies that investigate first, in real time, requiring additional authentication only as needed, versus automatically blocking access
- Enables PSPs to improve risk strategies and fine-tune policies without additional resources
- Eases compliance and elevates security posture for new and evolving regulatory requirements without disrupting existing processes
- Employs a sustainable security model that provides granular control over all roles and rules, and delivers on-demand audit trail for all records
- Correlates critical security data from all sources across entire internet payment services ecosystem, ensuring that no significant incident or event gets buried

Conclusion

Given the various internet payment services recommendations and guidelines issued to date (see sidebar: European Regulatory Initiatives for Securing Internet Payments), it is important that banks, PSPs, and other market participants anticipate the requirements of PSD2—the most recent and comprehensive regulations to date—including mandates regarding transaction monitoring and authentication.

Also critically important is the fact that the more stringent security standards of PSD2 will be translated into law and become mandatory for all 28 EU Member States by 2017. The level of compliance with the ECB recommendations and PSD2 will reveal each EU nation's commitment to combatting online payment fraud, enhancing customer trust, and harmonizing internet payment security across Europe.

European Regulatory Initiatives for Securing Internet Payments

Payment Services Directive (PSD): Directive administered by the European Commission to regulate payment services and PSPs throughout the EU, providing the legal foundation for the creation of a single retail payments market, effective 2008

Recommendations for the Security of Internet Payments, European Central Bank (ECB): Recommendations developed by the European Forum on the Security of Retail Payments (SecuRe Pay), effective February 2015

Guidelines on the Security of Internet Payments, European Banking Authority (EBA): Nearly identical guidelines providing a legal basis for consistent implementation and regulation of the ECB recommendations across the European Union, effective August 2015

Payment Services Directive (PSD2): Mandatory measures adopted by the European Parliament and EU Council of Ministers that will be translated into national law by EU Member States, effective 201

For more information, please visit www.vasco.com/irm

About VASCO

VASCO is committed to providing convenient, cost-effective technologies to secure the online community. Our practical integrated solutions are designed to address the most urgent fraud and risk management issues associated with internet payment systems. VASCO's versatile portfolio of cybersecurity solutions allows banks and PSPs to focus on their core competencies while providing them with a unique competitive advantage that can lead to increased market share and revenue.

Rely on the combined proven expertise of thousands of successful strong authentication deployments worldwide. Partner with VASCO to effectively address the ECB recommendations and prevent fraud. In addition to IDENTIKEY Risk Manager, the newest powerful weapon in a broad risk management and fraud prevention portfolio, VASCO is a global leader in authentication, digital signatures and identity management. Visit www.vasco.com to learn more about innovative technologies you can deploy to expand your security capabilities and return on investment, reduce monetary loss from fraud, and ensure compliance with evolving regulatory requirements.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com

VASCO®
THE AUTHENTICATION COMPANY