ozone API

The Verification Of Payee Rulebook Simplified

Contents

01. Introduction

Verification Of Payee (VOP) is a real time service that checks whether the name on a payment matches the actual account holder before money is transferred. It prevents both innocent mistakes and sophisticated fraud before they happen.

When a customer makes a payment, their Payment Service Provider (PSP) instantly queries the recipient's PSP to verify the name matches. The results are either Match, No Match, Close Match, or Cannot Verify, depending on the IBAN check. This appears immediately, allowing customers to catch errors or fraud attempts before confirming the payment.

This isn't optional anymore. VOP is rapidly becoming essential payment infrastructure across Europe, driven by a regulatory deadline of October 9th, customer protection requirements, and the escalating cost of authorized push payment fraud.

The numbers are compelling. Authorised push payment fraud cost UK PSPs £460 million in 2023 alone , while payment errors and misdirected funds create additional operational costs and customer friction. Early VOP implementations show 60-80% reduction in successful fraud attempts and significant decreases in payment errors. To help you navigate VOP, we've taken the complex EPC Rulebook and simplified it into an easy and accessible summary.

This rulebook includes:

- **Foundation:** Understand VOP and the key benefits
- **Legal Framework:** Legal requirements, contractual governance, and registry
- **Technical Implementation:** How VOP works and technical standards
- **Operational requirements:** Standards, compliance and risk requirements
- **Governance:** Scheme management and change control

02. Foundation

What is Verification Of Payee (VOP)?

VOP is a payment verification service that allows Payment Service Providers (PSPs) to check whether the name provided by a payee matches the actual account holder's name before processing a payment. This helps reduce payment errors and fraud.

Key benefits:

- Fraud Prevention: Reduces authorised push payment fraud
- Error Reduction: Catches payment mistakes before they happen
- Consumer Protection: Gives payees confidence their payment will reach the intended recipient
- Regulatory Compliance**:** Helps PSPs meet growing regulatory expectations

03. Additional Optional Services

Beyond basic VOP verification, PSPs can offer additional value added services (AOS) to enhance the customer experience and create new revenue opportunities.

Two types of additional services:

Individual PSP services:

- Value added services that individual PSPs offer to their own customers
- Built on top of basic VOP functionality

Examples include: Enhanced fraud monitoring, payment advice, account validation services.

Community services:

- Services offered collectively by groups of PSPs
- Can be local, national, or pan European initiatives

- Require transparency and public disclosure
- Must not create barriers to competition

Key rules for AOS:

- Must not compromise VOP interoperability or create unfair competitive advantages
- Should evolve based on market needs and customer demand
- Community AOS must be transparent with public disclosure requirements
- EPC may incorporate commonly used AOS features into the main scheme rulebook
- Cannot conflict with core VOP scheme requirements

04. Legal Requirements for Participation

4.1 Binding nature of the rulebook

The VOP Rulebook becomes legally binding through the Adherence Agreement that each participating PSP must sign.

Key legal principles:

- Participants remain fully responsible even when using intermediaries or outsourcing VOP services
- Covers both inter-PSP relationships and minimum requirements for PSP-customer relationships
- Creates binding obligations that can be legally enforced
- Establishes clear liability and responsibility frameworks

Responsibility chain:

- PSPs cannot transfer liability to third parties
- Outsourcing arrangements must maintain compliance
- Participants must ensure all intermediaries follow rulebook requirements

4.2 Infrastructure and competition framework

Single rulebook, multiple infrastructure providers - this is a key design principle of the VOP scheme.

How it works:

- One standardized rulebook governs all VOP operations
- Multiple technical infrastructure providers can offer VOP services
- Market forces determine which infrastructure PSPs choose
- Results in consistent scheme operation across different technical platforms

Benefits:

- Promotes competition among infrastructure providers
- Gives PSPs choice in technical solutions
- Maintains interoperability across all platforms
- Reduces dependency on single providers

4.3 Contractual governance

Legal framework:

- Belgian law governs the VOP Rulebook
- English language version prevails over any translations
- Document hierarchy established for resolving conflicts between different scheme documents

Statute references:

- References to legislation include future amendments
- Participants must comply with updated regulatory requirements
- No grandfathering of outdated regulatory versions

Conflict resolution:

- Clear hierarchy determines which document takes precedence
- Rulebook provisions override contradictory bilateral agreements
- EPC has final interpretation authority

4.4 EU Legislation application

Geographic scope and compliance:

- Must comply with PSD2 equivalent obligations
- Subject to same regulatory standards as EU PSPs
- Must demonstrate comparable regulatory oversight

National law conflicts:

- Participants should avoid exercising national law rights that conflict with PSD2 requirements
- EU law principles take precedence in cross border transactions
- National implementations must not undermine scheme interoperability

Expansion criteria:

- Geographic scope expansion follows specific criteria
- New jurisdictions must demonstrate regulatory equivalence
- EPC evaluates legal and technical compatibility

4.5 Intellectual property rights

EPC owns full copyright to the VOP Rulebook and all related scheme materials.

Key IP rules:

- EPC retains all rights to rulebook content and updates
- Participants cannot assert contrary ownership claims
- No infringement of EPC's copyright permitted
- Licensing terms govern participant usage rights

4.6 Official participant registry

EPC maintains an official registry of all PSPs and institutions participating in the VOP scheme.

Registry contents:

- Current contact details for all participating PSPs

- Participation start dates and any removal dates
- Operational data needed for transaction routing
- Technical connectivity information
- Geographic scope and service availability

Publication requirements:

- Participants consent to publication by applying to join the scheme
- Registry is accessible to all scheme participants
- Changes must be provided according to scheme management processes
- Updates must be made within specified time frames

Data management:

- Registry maintained by EPC Scheme Management Office
- Regular updates ensure accuracy
- Participants responsible for notifying changes
- Used for transaction routing and dispute resolution

05. How Verification Of Payee Works - Technical Process

5.1 Basic 5-Step process:

- Customer initiates payment with payee name and account details
- Requesting PSP sends VOP query to responding PSP
- Responding PSP checks name against account holder
- Response sent back (Match/No Match/Close Match/No Response Possible)
- Requesting PSP informs customer and processes payment accordingly

5.2 Response categories:

Match: Name matches exactly or very closely
No Match: Name clearly doesn't match
Close Match: Partial match that might be correct
No Response Possible: Cannot verify (e.g., account closed, restrictions)

06. Technical Standards and Data Requirements

6.1 Technical naming conventions

Standardised codes ensure consistency across all VOP documentation and implementations.

Process codes:
PR-xx: Main processes (e.g., PR-01 for the core VOP verification process)

Process-Step codes:
PT-xx-yy: Individual steps within processes
Example: PT-01.01 = First step of main VOP process

Dataset codes:
DS-01: VOP Request Dataset
DS-02: VOP Response Dataset
DS-03: Error/Exception Dataset
DS-04: Routing/Directory Dataset

Attribute codes:
AT-Exxx: Payee-related attributes (e.g., AT-E001 for Payee Name)
AT-Dxxx: Requesting PSP attributes
AT-Rxxx: Response-related attributes
AT-Txxx: Transaction-related attributes

Usage requirements:

- All technical documentation must use these standardised codes
- Infrastructure providers must implement consistent code usage
- Ensures interoperability between different technical platforms

6.2 Required data standards

Usage requirements:

All technical documentation must use these standardised codes
Infrastructure providers must implement consistent code usage
Ensures interoperability between different technical platforms

6.2 Required data standards

VOP Request must include:

AT-E001: Payee Name (as provided by payer)
AT-E002: Payee Account Identifier (IBAN)
AT-D001: Requesting PSP Identifier
AT-T001: Transaction Reference
AT-T002: Request Timestamp

VOP response contains:

AT-R001: Verification Result (Match/No Match/Close Match/No Response Possible)
AT-R002: Response Code
AT-R003: Response Timestamp
AT-T001: Original Transaction Reference

6.3 Data protection requirements

- Minimal data sharing (only name and account number)
- No transaction amounts or sensitive details shared
- 24-hour data retention limit for VOP data
- Purpose limitation: Data only used for verification

6.4 Technical implementation requirements

Technical standards:
- ISO 20022 messaging format requiredAPI based connectivity recommended
- Real time processing capability needed
- Fallback procedures for technical failures

Operational standards:
- 24/7/365 availability target
- Sub second response times for most queries
- Comprehensive logging and monitoring
- Incident management procedures

Security requirements:
- End to end encryption for all VOP messages
- Strong authentication for system access
- Regular security assessments
- Fraud monitoring capabilities

07. Participant Obligations

7.1 Requesting PSPs must:

- Display results clearly to customers
- Allow customer choice on how to proceed
- Report scheme wide risks and major incidents
- Maintain appropriate business continuity arrangements
- Screen information to prevent misuse
- Have specific dispute resolution requirements
- Detailed reporting obligations for scheme wide risks and major incidents
- Requirements for RVM agreements and oversight
- Follow Know Your Customer requirements for Requester agreements

7.2 Responding PSPs must:

- Respond within time limits (typically real time)
- Ensure accurate name matching
- Protect customer data and limit retention
- Handle disputed verifications appropriately
- Provide 24/7 service availability
- Maintain audit trails for regulatory compliance
- Have specific requirements for RVM oversight
- Have detailed data processing and storage limitations
- Follow requirements for handling disputed verifications

08. Implementation Requirements

8.1 Operational standards:

- 24/7/365 availability target
- Sub second response times for most queries
- Comprehensive logging and monitoring
- Incident management procedures

8.2 Ongoing compliance:

- Regular compliance reporting to EPC
- Performance monitoring and improvement
- Customer complaint handling
- Regulatory coordination with national authorities

8.3 Risk management requirements

PSPs must:

- Monitor for scheme wide risks and major incidents

- Report issues immediately to EPC
- Maintain appropriate business continuity arrangements
- Coordinate with other participants on risk mitigation

09. Scheme Management and Change Control

9.1 EPC Governance structure:

- Payment Services Management Body (PSMB) provides oversight
- Scheme Management Office handles day to day operations
- Regular rulebook updates based on market needs
- Stakeholder consultation on major changes

9.2 Change management process:

- Major changes: Require extensive consultation and approval
- Minor changes: Streamlined process for technical updates
- Exceptional changes: Fast track for urgent regulatory requirements
- Regular publication of updates and timelines

9.3 compliance monitoring and enforcement:

- Compliance monitoring by EPC
- Remedial action procedures for non compliance
- Suspension/exclusion mechanisms for serious breaches
- Financial penalties for scheme rule violations

ozone API

The Verification Of Payee Rulebook Simplified

www.ozoneapi.com