paladin vendor report | payment systems

paladingroup | RPGC GROUP

Welcome to the 2021 the Paladin Payment Vendor Report.

The mission of the Merchant Risk Council (MRC) is to provide members with useful tools and hard-to-find information that's critical to managing payment infrastructure and improving the customer purchasing experience. At the MRC, we understand how difficult it is to navigate a complex ecommerce environment and find the right solution for specific payment needs. As a benefit of your MRC membership, we are offering members a discounted copy of the Paladin Vendor Report (PVR).

The PVR, gathered by the industry experts at Paladin Group, provides detailed information about seven top Payment Switch vendors who offer a wide variety of different tools, platforms, and services. This report is designed to give you a comprehensive overview of the different products offered by each company—and to present analysis to help you focus on who may ultimately best align with your organization's payment management goals.

We hope you find this report to be a helpful resource that will provide you and your business with valuable insights. We are also interested in hearing your feedback on the report and encourage you to send any comments directly to programs@merchantriskcouncil.org.

Sincerely,

The MRC

Table of Contents

Introduction

Every day, we at Paladin Group are in the thick of the fast-paced world of fraud solutions. After all, ecommerce fraud is the top payments challenge according to the Merchant Risk Council's Global Payments Survey. Payments and fraud have never been more intertwined since more companies are deploying omnichannel solutions and Europe's strong customer authentication mandate is now in effect. That's why we've enlisted the authors of this report, Retail Payments Global Consulting Group, to help map the current payments technology ecosystem.

2020 unveiled paradigm shifts in how payments products are sold to merchants. "Payments orchestration" became an SEO buzzword. Payment Service Providers (PSPs) continue to tout their smart routing engines, network token services, and decline retry capabilities. While the years go by, one constant remains true, no one single vendor can fully service every market. Most enterprise merchants will use a combination of the vendors featured in this report, whether they be PSP, gateway, billing engine, token vault, or payments orchestration platform.

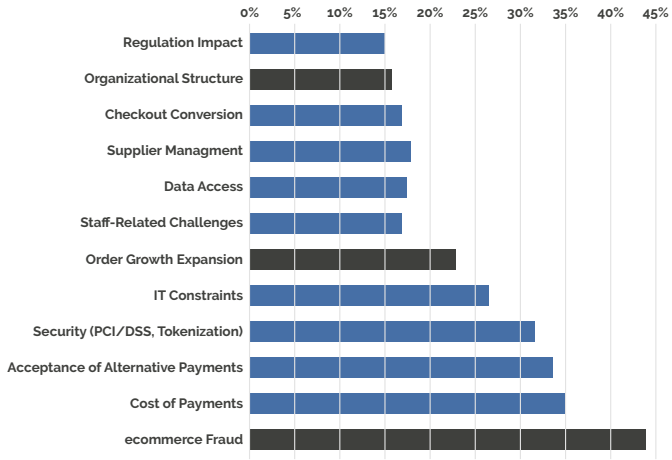


Figure 1: Payment-Related Challenges Ranked

Source: MRC and Cybersource's Payment Management Strategies of Forward-Thinking Global Merchants Global Payments Survey.

As demonstrated by Figure 1, merchants' top payments challenges are the cost of payments, the acceptance of alternative payments, security, and IT constraints.

Thanks to a fragmented token environment from providers and continuously changing card scheme compliance requirements, the

We focused on several key areas during the discovery process. (Not all are applicable to every vendor, but for consistency, we examined each of the following wherever relevant.)

FUNCTIONAL ARCHITECTURE - What the platform's capabilities are such as transaction types and value-added services.

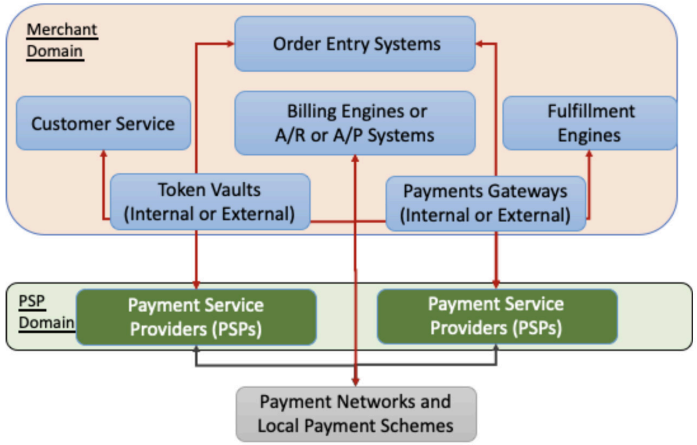
TECHNOLOGY - The platform's physical attributes such as technologies used, locations, and APIs.

CUSTOMER SUPPORT - What self-service tools and account management availability augument the platform.

PRICING MODEL - Usage of the platform is typically billed in either a per transaction, subscription, or licensee fee.

challenges of implementation and maintenance have also increased. Operating payments within multiple merchant systems creates a complicated web of interactivity just to maintain a single PSP relationship and handcuffs operations (see Figure 2). This type of environment is not the best practice, regardless of whether it's built or bought.

Figure 2: A Complicated Web of Payments Interactivity



Source: The Need for Payments Orchestration. Presented to Merchant Advisory Group Dec. 2019 by Rene Pelegero (RPGC Group) & Suhil Srinivas (LinkedIn).

The companies featured in this report help merchants address those concerns. We see three philosophies at work: pure technology plays, pure Payment Service Providers, and hybrids.

In previous versions, this report has solely focused on Payment gateways/switches/hubs. They were pure technology plays. These platforms now assume a new moniker: payments orchestration platforms, or POPs. To meet our definition of payments orchestration, the platform must support all processing connections through a single API, support dynamic routing (also known as cascading) without additional code, provide an end-user tool to configure routing rules, and provide the necessary data elements to log and audit the state of each transaction. POPs argue that their solutions are the most straightforward and that the best architectural solution is to abstract the payments layer to the periphery of the core technology stack. These vendors only provide technology and do not assume financial ownership of the transactions on their platforms.

Payment Service Providers address the other two other approaches of increasing authorization approval rates and lower payments costs. For simplicity moving forward, any entity that takes fiduciary responsibility of transaction processing such as an acquirer, a third-party provider, or a payment service provider, will be referred to as a PSP. PSPs have worked for years to create solutions to provide all services to all merchants. For the first time they are now featured in this report.

PSPs provide a vital role to the payments ecosystem. Enterprise merchants still need a great deal of the functionality PSPs employ today. But PSPs have demonstrated economic bias to control all of their clients' volume. This has led many merchants frustrated by their providers when they need a specific connection or license that then forces the merchant into a new configuration to achieve PCI compliance and reconciliation.

The highly-respected and appropriately staffed merchants partner with several PSPs in order to maximize market coverage and mitigate the potential damage outages and fraud can create. Thus, the term "layered approach" isn't just for fraud anymore. PSPs like Checkout.com, Nuvei, and Fiserv recognize this fact, and have opened up their platforms to meet this market demand as they seek to straddle the line between a walled garden and an independent orchestration platform. This new hybrid approach is what opened the scope of this year's report.

In addition to the term PSP, there are some other formatting and acronyms to keep in mind for this report.

- API - Application Programming Interface
- SDK - Software Development Kit
- POS - Point of Sale
- APM - Alternative Payment Method
- PAN - Primary Account Number
- CNP - Card Not Present
- PCI - Payment Card Industry Data Security Standards
- SAQ - Self-Assessment Questionnaire
- 3DSX.X - 3D-Secure version X.X
- HSM - Hardware Security Module
- UUID - Universally Unique Identifier
- SLA - Service Level Agreement

Any text in `this_format` or `thatFormat` represents specific code or data fields.

The vendors featured in this report seek to address the challenges of safely managing a global payments platform. Each platform is reviewed for functionality, technical capabilities, customer service, and pricing model. These considerations are top-of-mind for any merchant deliberating the "build or buy" question.

Neither Paladin nor RPGC has written any opinions, given any reviews, or displayed any thumbs-up (or down) about the vendors contained in the report. This report is not designed to rate the products and services of the vendors—its intent is to provide clarity regarding the products and services available.

We've prepared materials on 36 companies providing services in this space. Each vendor had the option to participate in the report, and we were compensated for our time by those who elected to participate. Our team spent hours in discussion with each of these

participants. We test-drove their products and gathered overviews of their services, marketing, sales, technologies, products, and future plans.

For vendors who chose not to participate in the report, we drew upon client input, research, and interview where available to share a summary of their services. If a vendor did not have publicly available API documentation nor made themselves available for a demo, they were not included. This report documents an effort to gain as much first-hand knowledge as possible from payment switch vendors, compiling our findings in a way that's helpful and revolutionary for our industry and the merchants who depend on us.

Core functionality icon key

Dynamic Routing—Also known as Cascading or fallback routing. The ability to reroute a transaction from one acquirer to another without notifying the customer of an issuer decline

Smart Routing to Maximize Approvals—The ability to supply their own proprietary algorithms to route transactions to maximize authorization approvals on a Client's behalf without the need for further code development.

Smart Routing for Least Cost—The ability to supply their own proprietary algorithms to route transactions to maximize cost savings on a Client's behalf without the need for further code development.

Configurable Transaction Routing Tool—The ability to expose business-user friendly tool to route transactions using arbitrary business logic in the Client dashboard. This means users can develop decline retries trees or logic to route transactions according to transaction attributes without the need for additional programming.

Dynamic Statement Descriptor—The platform allows clients to configure descriptors presented on a customer's card statement on a transaction by transaction basis

Split Tender Transactions—The ability to receive a single payment request from the merchant and split it into multiple transactions using different cards, payment methods or loyalty programs. While partial authorizations are a form of split tender transactions, only the platforms that enable a transaction using multiple instruments qualify for this criteria.

Partial Captures—The ability to submit the same transaction for clearing multiple times for customizable amounts.

Reporting—The provider offers a dashboard or API that can be used to analyze activity in a Business Intelligence tool.

Passess Raw Issuer Decline Codes—The platform's API returns the issuer's decline codes without normalizing the response codes or obsfuscating them under technical error codes.

Automatic Reversals—The ability to automatically initiate the release of an authorization upon arbitrary criteria before capture.

Supports Push Payments—The ability to disburse payments to bank accounts, e-wallets, and payment cards OR the ability to accept payments using the Request-To-Pay protocol.

Custom Alerts—Platform has the ability to send Client notifications when Client-set business rule thresholds are exceeded

Provides Endpoint Latency—The ability to report an API endpoint latency in milliseconds and use that latency as a routing rule.

Ingests and Consolidates Settlement Reports—The ability to normalize data from various reports and displays to user in a single interface.

Network Token Requestor—Certification with at least one EMVCo member's Token Requestor programs to request and share network tokens across multiple Clients and partners. Vendor must also be capable of storing and transmitting Payment Account Reference number to Clients.

Tracks Event States—The platform leverages real-time ledgers or event states as a means of tracking a transaction through the platform

Account Updater integration—The platform is able to perform Visa Account Updater and Mastercard Billing Updater regardless of the client's acquirer agreements.

Dynamic Payment Method Presentation—The ability to selectively present specific payment methods on the checkout page to the end-customer by product type or geography to maximize checkout conversions.

A/B Testing Suite—The platform provides clients a tool to make and track payments related tests.

Homegrown 3D-Secure 2 Server—Vendor has developed its own EMVCo certified 3D-Secure 2 Server.

Homegrown Fraud Decision Engine—The company also offers a fraud mitigation platform that is integrated or developed into the platform.

IXOPAY

Developed in 2016, the **IXOPAY** platform is a scalable and PCI-certified payment orchestration platform for whitelabel clients and enterprise merchants. The extendable architecture provides user-configurable tools to intelligently route transactions, manage risk rules, automate reconciliation, and ingest settlement reports.

IXOPAY services more than 2,000 clients selling delivery services, retail, digital goods, insurance, payment facilitation, and asset trading (both stocks and cryptocurrencies). In 2020, the Adapter list grew from forty-five to ninety integrations, including Apple Pay and Google Pay.

Successful coordination of payment operations, both technical and organizational, requires a level of automation that **IXOPAY** seeks to provide for its clients—regardless of how technically disparate a client's back office system may be. **IXOPAY's** product investments are informed by the need to help their clients justify an ROI to improve processes. Using **IXOPAY**, clients can prove ROI by:

- Reducing costs by using an integrated platform for Transaction Processing, Risk Management, Post-Processing (settlements and reconciliation), and reporting.
- Reducing costs by automating developer-intensive processes such as the development of payment integrations, reconciliation, or mass configuration. Some of IXOPAY's reference clients have reduced the manual effort related to payment processing within their teams by up to 75%.
- Increasing revenue while reducing costs by providing clients the tools to optimize for payment KPIs (such as authorization approval rates and payment fee ratios) through the platform's built-in functionality.

At a Glance:

The specific ways in which **IXOPAY** improves ROI will differ from client to client, but it is always fundamentally linked to the deep functionality, high degree of automation, and configurability offered by **IXOPAY** and the cost-saving potential enabled thereby.

Based in Vienna, Austria, **IXOPAY** employs over thirty people between their offices in Vienna and Orlando, FL. **IXOPAY** is a subsidiary of the IXOLIT group with sister services including IXOPLAN (a subscription billing engine), IXOCREATE (a content management system), and IXOCARE (a call center platform).

Functional Architecture

IXOPAY was designed to manage payments through one API integration. The core functionality is accessible through the Transaction API, which enables transaction requests, status requests, transaction scheduling, and handling for successful transactions and errors. Once an integration with a master merchant or PSP is complete, sub-merchants can onboard into a client environment using the portal's "Merchant Configuration" tool.

The Transaction API supports eight transaction functions:

- Debit (authorize + capture)
- Preauthorize (**IXOPAY's** term for authorization)
- Capture
- Void
- Refund
- Payout
- Register (used in conjunction with pre-authorizations and debits to save payment methods)
- and Deregister

The use of each transaction function returns a unique ID. The API supports full redirects (e.g., to Paypal) and hosted payment forms (with or without iFrames). Using an asynchronous payment flow, external system messages are canonically converted into **IXOPAY's** native message format before manipulation within the **IXOPAY** platform and posting directly into the client's ERP system for reconciliation. The Javascript library and gateway documentation are publicly available.

Routing Engine

IXOPAY uses the concept of connectors to enable its routing engine and to set up MIDs for processing. A connector implements the connection between the merchant account and the adaptor endpoint (e.g., a payment method). Connectors can be configured to affect specific sub-merchants, products, geographies, or business lines. In addition, connectors can be assigned risk profiles. Most importantly, each connector can be assigned risk rules and transaction routing rules.

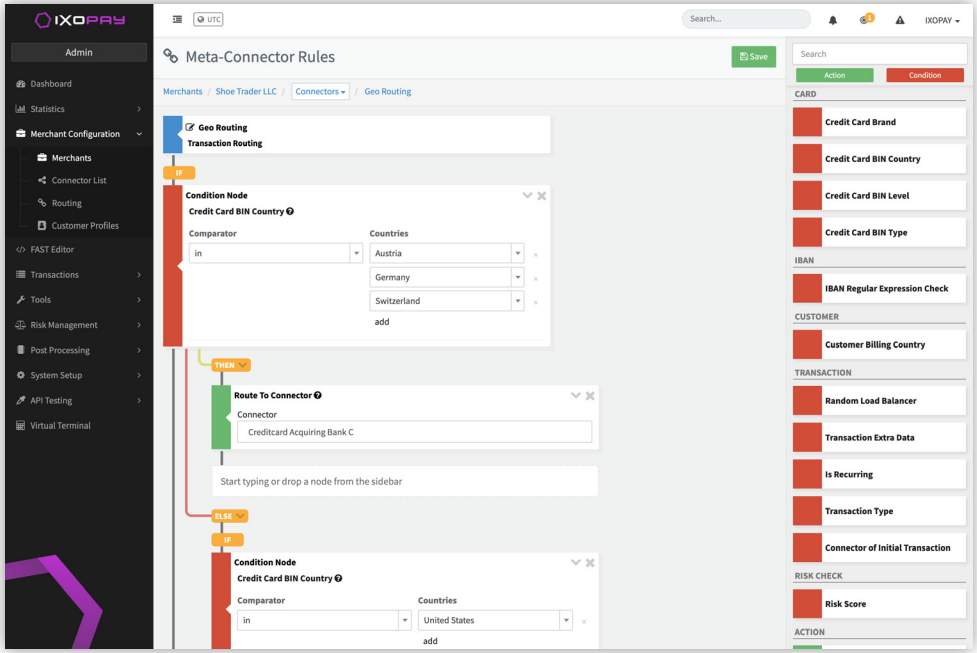


FIgure 1: **IXOPAY's** Smart Transaction Routing Tool

To orchestrate transactions, **IXOPAY** uses the concept of MetaConnectors to determine risk, routing, and payment method presentation rules. To optimize and test routing strategies, users build decision trees using drag-and-drop "if/then/else" rules in the Routing tool. Routing is configurable by BIN, IBAN, customer country, risk score, chargeback ratio, currency, transaction type, or custom merchant input. Using the custom extra data input, clients can pass additional data input, such as a third party pre-authorization blocklist check through the Transaction API to enable or disable specific routing paths.

This MultiMethod approach can be used to define the total set of payment methods a merchant may want to present to a customer based on submerchant, customer IP address, transaction currency, and risk score. Thus, an **IXOPAY** client can simplify their payment method management with the Routing tool to ensure that customers are presented the appropriate payment methods at checkout .(e.g., a customer from the United States will never be presented SEPA Direct Debit on an **IXOPAY** hosted checkout).

Risk Management

The Risk Rules engine allows clients to build and apply Risk Profiles to meet different payment flows (e.g., payouts, SCA exemptions, blocklists). **IXOPAY** supports custom parameters to define the risk scores for forty different rule types. These rules include checks on velocity, device location, and deviceID. As with any fraud rules engine found in the Paladin Vendor Report, **IXOPAY** allows clients to assign risk score weights that can be measured against a scorecard to determine whether or not to approve a transaction, send a transaction to manual review or 3D-Secure, or decline a transaction. The risk score **IXOPAY** uses to route transactions does not necessarily need to come from the Risk Management Rules Engine as **IXOPAY** supports integrations with Kount and Notolytix to ingest their risk scores. And as stated before, **IXOPAY** can also support routing conditions from custom data inputs from fraud

vendor integrations outside of the IXOPAY ecosystem, but additional setup is required.

Outside of the rules engine itself, IXOPAY also supports some other fraud prevention functionality. The platform manages its own blocklist and allowlist. Customers can upload their own lists, whether they be self generated or populated by third party service checks. These lists can be set up on single merchant accounts or across the entire organization. For EMV 3D-Secure, **IXOPAY** white-labels an EMVCo approved 3D-Secure 2.2 Server and a 3D-Secure 1 MPI so that its clients can directly transmit authentication requests to the Directory Server using client-defined criteria.

Despite having a sister company, **IXOPLAN**, a subscription billing engine, **IXOPAY** can support recurring payments and free trial periods. The gateway has a scheduler that enables recurring debits. Transactions are flagged on first- time transactions, which areis also used for filtering SCA transactions between Customer Initiated and Merchant Initiated card on file transactions. To support transaction optimization, **IXOPAY** added direct connections for the Visa Account Updater and the Mastercard Billing Updater in 2020. Support for the American Express Card Refresher is expected in 2021.

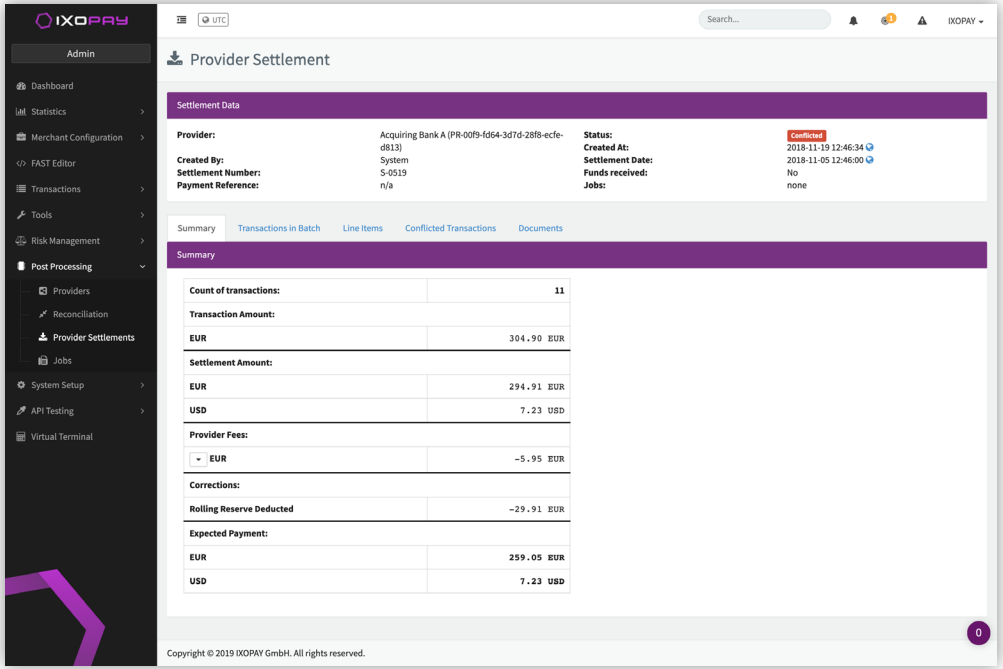


Figure 2: Reconciling Unknown Transactions in **IXOPAY's** Post-Processing Fee Engine

Post Processing Fee Engine

Because **IXOPAY** is sold to merchants and payment service providers, it provides a suite of settlement and reconciliation functionality. Settlement reports are directly ingested, parsed, and normalized into the **IXOPAY** Post Processing Fee Engine from adaptors. Reconciliation can be performed within the platform or fed to a third-party BI tool using the BI Data Source API. Within the platform, **IXOPAY** allows clients to compare their fees as described

in their merchant agreements with the fees they are charged in their settlement reports. The values **IXOPAY** uses to qualify fee rates to compare against settlement reports are created from logging Transaction API requests. Users can configure the engine to calculate interchange, scheme fees, markup, transaction fees, and one-time fees like monthly charges across all their providers. Transaction mismatches found from inconsistent transaction states can be manually reconciled.

The Post Processing Fee Engine also allows **IXOPAY** to ingest transactions initiated outside of the **IXOPAY** platform (e.g., transactions initiated from a PayPal dashboard but no redirect from **IXOPAY**). Extract, Transfer, and Load jobs can also be configured within the platform to transfer records to a client's ERP.

The dashboards, powered by ElasticSearch, are customizable by user, by user type, by merchant, and by any combination of those variables (e.g., the CFO of a submerchant or a payOps team for a holding company). Users can add and rearrange dashboards using templates to build widgets. The Pivot Table feature allows **IXOPAY** clients to track A/B tests within the platform by account, by merchant, by connector, and by various payment related dimensions over a granular period of time. Using this methodology, a merchant can set up a routing test and the required reporting to track the test in minutes. Pivot calculations can be performed to account for several submerchants to evaluate a corporation's entire portfolio.

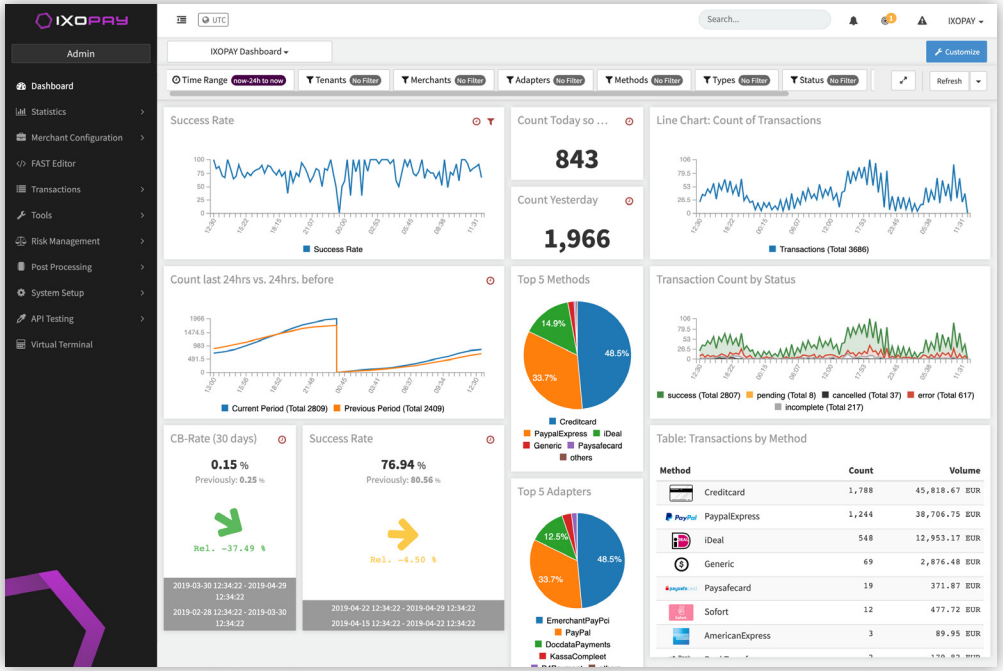


Figure 3: **IXOPAY** Landing Page Dashboard

Technical Architecture

The **IXOPAY** platform was designed for transaction matching and reconciliation. It sends the client an asynchronous notification once a transaction (each has a Unique ID, or UUID) reaches a final state. Each transaction state is assigned a UUID, whereas each transaction is assigned a specific purchaseID. This notification is designed to act as a merchant's source of trust when dealing with asynchronous transactions involving redirects. To prove the authenticity of the

notification, the Gateway signs every request with the same shared secret as used for signing your requests.

IXOPAY states that its platform is both synchronous and asynchronous. The platform chooses which flow to use based on the payment method and adapter in use (e.g., cards use synchronous flows, while boletos and redirects use asynchronous flows). Each transaction status change always sends a notification XML to **IXOPAY's** callback URL for asynchronous status notifications. With cards now adopting asynchronous requirements for SCA, these notifications are the basis for informing routing strategies on 3D-Secure retries.

Each transaction supports idempotency through a duplicate check that occurs on inbound and outbound transactions. The soft duplicate check, hard-coded into the platform, checks to see if a transaction request was previously used on outbound transactions. A strict check is performed on inbound transactions.

IXOPAY offers customers four integration options:

1. A full-page redirect to an **IXOPAY**-hosted payment page
2. An embedded **IXOPAY**-hosted payment form
3. A payment.js javascript library integration with sensitive fields for PAN and CVV rendered within iFrame fields hosted by **IXOPAY**
4. Server-to-server for recurring payments, refunds, captures, and voids that can also be used for SEPA direct debit since IBAN and BIC do not fall under PCI compliance

IXOPAY encourages enterprises to integrate into their payment.js Javascript Library for full styling and design on the checkout page. It renders two separate iFrames for card number and CVV so that a merchant can achieve SAQ-A while retaining control of the rest of their checkout page. In Github, **IXOPAY** provides SDKs for iOS and Android in-app tokenization.

Leveraging the full functionality of **IXOPAY's** platform requires integration into five REST APIs:

- Transaction API: Conducts client transaction requests and passes transaction data
- Schedule API: The Gateway's scheduler enables clients to perform recurring debits without any further intervention; based on the user-defined schedule, this API automatically triggers recurring transactions
- Status API: Allows clients to retrieve status of transactions and handle asynchronous postback notifications
- Push API: Allows clients to report transactions to the platform that were not processed by **IXOPAY**
- BI Data Source: Allows users to transmit payments data to a non-**IXOPAY** BI tool

API documentation and data objects are formatted in both XML and JSON for each payment method. Yet, there's a complete separation between outbound and inbound interfaces. Once inside the **IXOPAY** platform, resources and their objects are canonically converted into a common abstraction for processing. It is only when a transaction is transmitted outside of the **IXOPAY** platform that it is then converted into an XML or JSON object.

Unlike the majority of the vendors featured in this report, IXOPAY hosts its own data centers. They operate from two separate tier-three data centers in Vienna that are connected via redundant IXOLIT-owned dark fiber routes to provide automatic failover and full data synchronization every sixty seconds. Instances are also supported in Phoenix, Amsterdam, and Frankfurt. **IXOPAY** has joked that their data centers and client data could survive a blast from an 800 kiloton nuclear warhead.

IXOPAY is designed as a Multi-Tenant SaaS product. Customers are provisioned a master account with two master environments—sandbox and production. The master client is then able to partition tenants as they see fit through the dashboard. This tenant hierarchy allows **IXOPAY** clients to segment processing conditions and user permissions by geography or business line. Admin configurations can determine who has access and can monitor access through built-in audit logs. If the master tenant admin allows, each subtenant has full **IXOPAY** functionality and configurability.

Customer Support

IXOPAY assigns a Customer Success Manager upon signing a new client. The Customer Success Manager is directly supported by the technical team. To support integration, **IXOPAY** sets the client up as a master tenant, sets up a training workshop for operators, and provisions a user manual. The training workshop, a walkthrough of the portal tools, is designed for the entire client audience including product, operations, finance and engineers. The user manual provides walkthroughs and videos for each IXOPAY feature and function.

Users are provided self-service tools to implement new payment methods, routing tools and A/B tests. The customer success team provides blog posts, webinars, monthly client newsletters on new features, new connectors, and news updates.

The Network Operations Center (NOC) is **IXOPAY's** 24/7 technical support center. They have live monitoring on all transactions and tenants. Monitoring focuses on three aspects, the network, errors, and volume. NOC's network monitoring provides an overview of issues within **IXOPAY's** network and servers, helping prevent issues from impacting service. NOC has visibility of each tenant's incoming volume and each transaction error and failure, including information about the cause of the errors. If there is a rise in errors or failed transactions, then an investigation is triggered.

Each tenant is checked for changes or irregularities every ten minutes. If an irregularity is discovered, one NOC agent begins investigations while another agent contacts the 24/7 system administrator to establish contact within five minutes. The team is based in Vienna and has members fluent in English, German, Spanish, French, Dutch, Arabic, Mandarin, Russian, Romanian, Hungarian, Turkish, Serbian, Italian, and Polish.

NOC is tasked with identifying issues within thirty minutes and the team answers around 150 customer tickets per shift. During issues, customer success managers are the primary point of contact for clients, but that does not prevent NOC members from contacting clients about escalations when necessary.

Pricing

IXOPAY charges for its services using a per-transaction request pricing model. Onboarding costs can vary depending on whether the client opts for a white-label platform or an **IXOPAY** branded portal and documentation. There are minimal monthly fees for maintenance and support. Custom integrations can be priced and prioritized upon request.

paladingroup

Paladin would like to thank all of the participating vendors for their time and availability during the discovery and post-writing processes.

We also would like to remind all readers of this report that they can email us at info@paladinfraud.com to let us know which vendors they would like to see participate in the report next year.