

paladin vendor report | **fraud prevention**

2020



paladingroup



Thank you for downloading the Paladin Vendor Report.

The Merchant Risk Council's (MRC) mission is to provide members with useful tools and sometimes scarce information to help lower fraud and improve your customer's purchasing experience. At the MRC, we understand how difficult it is to navigate a complex ecommerce environment and find the right solution for specific fraud and risk 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, provides detailed information on over 40 vendors who offer a wide variety of different fraud prevention tools, platforms, and services. This report is designed to give you a comprehensive overview of the different products offered by each company and present analysis to help you focus on who may ultimately best align with your individual fraud prevention 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,

Markus Bergthaler
Director of Programs, MRC

The 2020 Paladin Vendor Report

Offering an unprecedented view into today's fraud prevention platforms and solutions

Every day at Paladin Group, we're in the thick of the fast-paced world of fraud solutions. As experts on today's solution providers, services, and tools, it's our job to maintain a high-level view of the fraud prevention landscape as well as a detailed, on-the-ground understanding of every solution and every challenge.

As the number of providers and services grow and technology evolves, merchants' options become increasingly complex and varied. Since it's our mission to serve as an authority on these products and their strengths, areas of opportunity, and enhancements, we published the first-ever Paladin Vendor Report (PVR) in 2017. It offered an unprecedented exploration of how merchants could mitigate the risks that come with accepting payments in an omni-channel, card-not-present world.

Because of the constant evolution of many popular fraud mitigation solutions, we decided to provide the Paladin Vendor Report on an annual basis. And now, we're pleased to publish the latest: the 2020 Paladin Vendor Report. We've offered previous participants the chance to update their sections and incorporated additional participating vendors.

The 2020 Paladin Vendor Report is purely informational. Paladin does not offer any opinions, reviews, or thumbs-up (or down) about the vendors contained in the report.

We focus 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.)

PRODUCT - The vendor's current functionality.

SERVICES - Available offerings to help merchants during integration and throughout their client lifecycle, including reporting.

BUSINESS DEVELOPMENT - Current partnerships and channels for direct and indirect customers.

MARKETING - The verticals vendors are focusing on and messaging

SALES - A breakdown of market segments.

TECHNOLOGY - How the product works from a technical perspective.

What this report offers: the PVR helps merchants navigate the ever-expanding number of solution providers and services available to them. We spoke with over 23 vendors who offer risk-mitigation products to merchants in the Card Not Present (CNP) and omni-channel environments—then gathered, examined, and compiled the information for each participating vendor. Vendors had the option to participate in the report, and Paladin was compensated for the research performed. Our team spent hours in discussion with each of these vendors—with many of these discussions taking place on-site. We test-drove their products and gathered overviews of their services, marketing, sales, technologies, and future plans.

For vendors who chose not to participate in the report, we drew upon our extensive interaction, client input, and research to share a summary of their services. This report is a groundbreaking effort to gain as much first-hand knowledge as possible from fraud prevention vendors, compiling our findings in a way that's helpful and revolutionary for our industry and the merchants who depend on us.

Again, this report is purely informational, and it is not designed to rate the products and services of the vendors. Its intent is to provide clarity regarding what products and services fraud-mitigation vendors offer. The vendors are segmented into six

different categories based on their core offerings. Some of the vendors offer other products that complement their core offering or have additional functionality or products. Some vendors provide services in overlapping segments, and this report offers a separate overview for each of the following categories:

- **User Behavior & Behavioral Biometrics**
- **3DS & Consumer Authentication**
- **Device Identification, Reputation, & Reputation**
- **Fraud Platforms & Decision Engines**
- **Identification & Data Verification**
- **Chargeback Management & Platforms**

Core functionality icon key

		
3rd Party API Capabilities	Payment Gateway Capabilities	Operational Support
		
Machine Learning	Guaranteed Chargeback Liability	ATO Detection Capabilities
		
Account/Client Management	Device Fingerprint Capabilities	Historical Sandbox Testing
		
Professional Guidance/Services	User Behavior Capabilities	Pre-Authorization Functionality
		
Fraud Engine/Platform Functionality	Non-Production Real Time Rules Testing	

3rd Party API Capabilities – The ability to call out via API to third-party vendors for data, device fingerprinting, etc.

Payment Gateway Capabilities – The ability to process payments directly through their own platform or solution.

Operational Support – Provides outsourced operational support, at a cost, for reviewing high-risk transactions and/or managing chargebacks.

Machine Learning – Matching algorithms to detect anomalies in the behavior of transactions or users.

Guaranteed Chargeback Liability – Guarantees merchants do not take fraud losses for vendor-approved transactions.

ATO Detection Capabilities – Using device characteristics to detect account takeover/account penetration.

Account/Client Management – Personnel dedicated to working directly with clients.

Device Fingerprint Capabilities – Built directly into the platform (not a third-party API call).

Historical Sandbox Testing – Ability to test rules against historical transactions in a non-production environment.

Professional Guidance/Services – Provides outsourced support for data analysis, rules-building, and recommended best practices, etc.

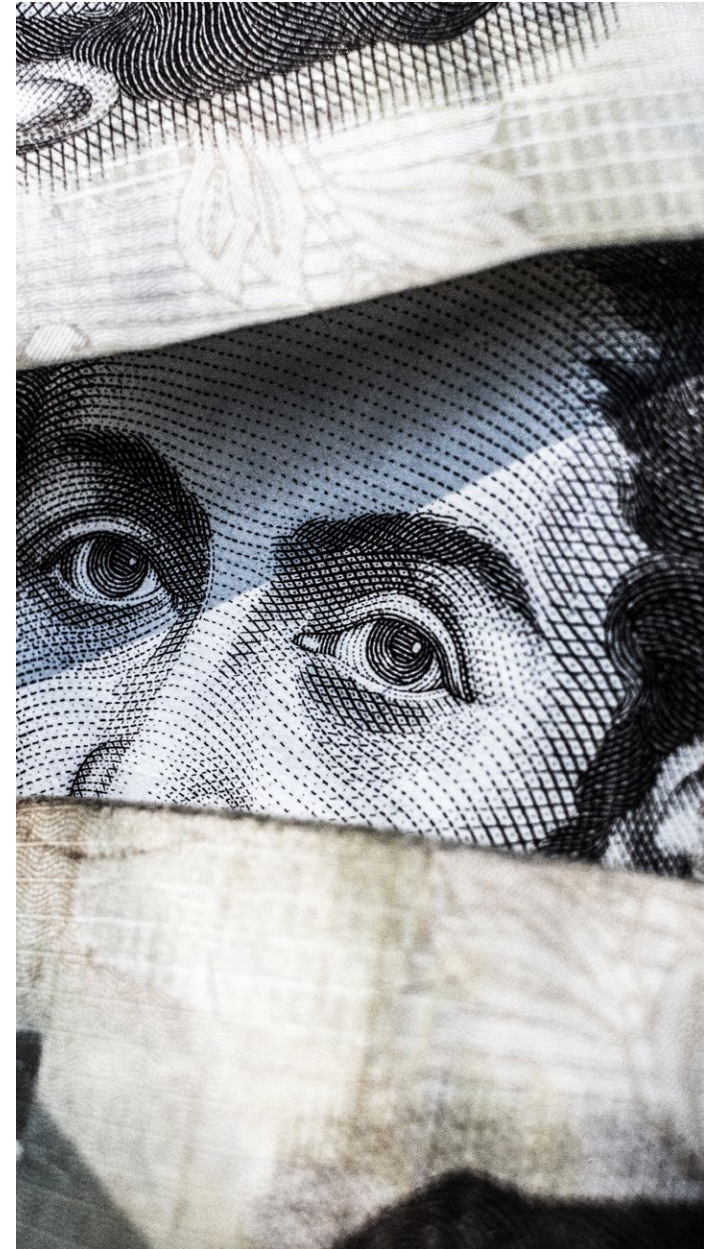
User Behavior Capabilities – Built-in (not via third-party) capabilities to capture cursor movements, mouse clicks, and time on a merchant site.

Pre-Authorization Functionality – Ability to score and/or decision a transaction prior to authorization.

Fraud Engine/Platform Functionality – Ability to score/decision a transaction post-authorization.

Non-Production Real Time Rules Testing – Ability to test real-time transactions in a non-production environment.

Third-party fraud prevention platforms provide protection and flexibility to not only prevent fraudulent transactions but also increase acceptance of legitimate orders. They help scale fraud teams by managing, or helping to eliminate, the manual requirement associated with transactional order review. Often, the foundation of the prevention platform is a customizable rules engine designed and maintained to identify historically high-risk combinations of order attributes, then make a decision on behalf of the merchant.



Arvato Financial Solutions

Arvato Financial Solutions is a global financial service provider and part of Bertelsmann SE & Co. KGaA as a subsidiary of Arvato.

The company has around 7,500 employees in 17 countries, including a strong presence in Europe, Brazil, and the U.S. They offer flexible full-service solutions for efficient management of customer relationships and cash flows. **Arvato Financial Solutions** is synonymous with professional outsourcing services centering on cash flow in all phases of the customer lifecycle – from risk management and invoicing to debtor management, the sale of receivables, and debt collection. As part of this, **Arvato** focuses on minimizing default rates in the business initiation phase and during the collection process. As a result, services also include optimizing the selection of payment types internationally.

As a financial solutions provider, **Arvato** manages around 10,000 customers, specializing primarily in the retail/ecommerce, telecommunications, insurance, banking, and healthcare sectors. This makes them Europe's third-largest integrated financial service provider.

Solutions & Functionality

Within the ID & Fraud Management segment, **Arvato Financial Solutions** offers solutions and services to prevent and detect fraud while allowing an optimized experience for legitimate customers. These services can be applied as an end-to-end solution, or as segmented modules depending on the client's need.

Merchants can utilize the **Arvato Financial Solutions** infrastructure as an approach to new markets as well—for example, when entering the European market with its unique payment and legal landscape. **Arvato Financial Solutions** uses a "make,



At a Glance:



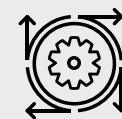
3rd Party API Capabilities



Payment Gateway Capabilities



Operational Support



Machine Learning



Account/Client Management



Device Fingerprint Capabilities



Historical Sandbox Testing



Professional Guidance/Services



Fraud Engine/Platform Functionality



ATO Detection Capabilities



User Behavior Capabilities



Pre-Authorization Functionality

partner, buy" strategy, bringing together the best technologies with regional, financial, and cross-industry expertise. This approach enhances customer trust and ensures that clients have access to the most sophisticated technology available to fight fraud. **Arvato's** solutions and modules operate in real time and in accordance with European data protection legislation.

These solutions include the following:

Device Fingerprinting helps clients identify and recognize a device based on different attributes such as device type, screen size, and user agent. These are gathered to generate a Device-ID. Specific device and transactional data can be put on client-specific blacklists or whitelists as device history is created. This record allows for recognition even if changes are made in the device itself through browser or operating system updates. The technology can also indicate a user's true geographic location and detect proxy servers which are known to be high risk. The association of diverse data types allows for detecting fraud attempts which would not be identified by a single variant.

Device Fraud Pool (DFP) improves fraud detection by providing access to a large database that makes it possible to compare device and transactional information. This is done on a rule basis along with other numerous records in the pool. It helps recognize transactions that seem valid but have been identified as fraudulent by other

clients. The rule-set is industry-specific to make it possible to detect industry-specific fraud. This solution can help detect fraudulent transactions earlier in the process and reduce false positives.

The **DFP** increases the value of **Device Fingerprinting** by sharing device and transactional data as input for the Fraud Rules Engine. These datasets from pool clients remain invisible to other pool clients since no transactional data is shared between the **DFP** clients.

Behavioral Biometrics analyzes device, location, and the user's signals to build an ongoing digital identity. The user is identified based on the individual passive biometric profile (such as user finger pressure, fingertip size, touch coordinates, device movement). The solution also allows clients to authenticate the user's navigation behavior during the web session (such as typing, clicking, zooming, and swiping) against historical and normal population patterns anonymously. This analysis informs clients of fraud risk and gives them advice regarding what actions to take. Not only does this serve to identify high-risk behavior and detect automation, but it also notes legitimate customers' behavior, which can help fast-track good transactions through the checkout process, which reduces potential customer friction. The service is applicable to both web and mobile applications (iOS, Android, Windows).

The **Fraud Rules Engine** is a core component of the fraud prevention and detection infrastructure, used to link all relevant data points. It can provide a multidimensional view of data collected, allowing for evaluation of the consumer's transaction. The **Fraud Rules Engine's** design adapts to a number of fraud issues by analyzing correlations on a large set of historical data.

The application of machine-learning algorithms can help complement the rule-based approach, while **Advanced Analytics** also help predict fraud and generate risk scores in real time. In this framework, a recommended action is suggested, and the decision whether to approve a transaction can take place automatically or manually. In conjunction with the **Fraud Management Cockpit**, customers can view triggered rules and manage blacklists and whitelists. Rules can be used across a user base, and the service team supports building new and specific rule sets together with the client.

The **Fraud Management Cockpit** allows clients to manually review transactions based on predetermined rule sets and score thresholds. Transactional data and all fraud check results are displayed in a customizable user interface. The ultimate goal is to provide enough in-depth detail to make a decision, in addition to providing the transparency to follow up on historical judgment without overwhelming the fraud analyst. The optional connection to a client's order-management system allows manual order

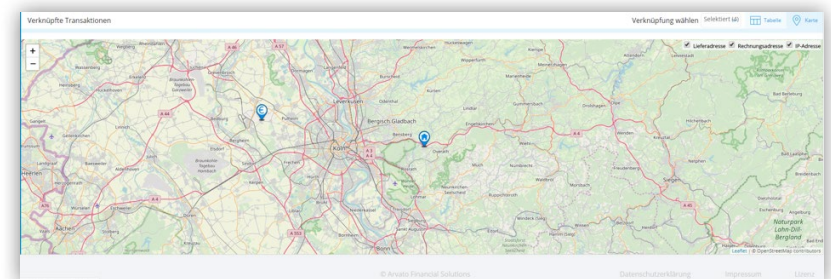
[illegible]

review results to be automatically transmitted into the client's order-management system. Examples of features in the response detail include geographical order location, overview of all linked transactions, and order handling recommendations.

Verkaufte Transaktionen Verknüpfung wählen: [Zurück](#) [Neu](#)

★
👤
👥
🛒
💬
📄
📧
📅

	Expiren	Status	Hersteller	Kommentar	Datum	Beziehnummer
📄	🟡	🟢			23.10.2019 10:07:17	yp1096214104
📄	🟡	🟢			23.10.2019 10:07:16	ab04854623764
📄	🟡	🟢			23.10.2019 10:07:15	ue0399477177
					21.02.2019 10:23:52	P06213130461



Through visualization of connected transactions within the interface, users can apply decisions on orders, add notes or comments, and tab through all relevant customer and order details (such as items, card info, etc.). Linked transactions can be viewed via matrix or linkage map, including potential secondary links. Users can add or remove criteria from the queue that is not relevant, and any changes or customizations to the individual review interface are persistent when logging in and out.

Users can also add or remove “widgets” designed to ingest order detail and track performance of certain rule configurations. Users are then able to search a list of all orders that contain those criteria, which can help track schemes and attacks in either the long- or the short-term.

Services Offered:

To further support the notion of end-to-end fraud solutions, **Arvato Financial Solutions** includes **Fraud Manual Review** outsourcing support among its services. These services are designed for clients who may not have the bandwidth for manual order review, or who may have a seasonal need during peak volume periods.

Arvato Financial Solutions' experienced fraud agents support in manual online fraud prevention with knowledge of country-specific and industry-specific fraud schemes and behavior. Decisions are generally taken directly, but in some ambiguous cases, consumers are contacted on behalf of clients. Thanks to an agnostic approach, it's also possible to fully orchestrate customer-specific tools. Based on the global coverage, the team provides "follow the sun" support 24/7/365 for global and regional clients.

Through their industry and global fraud experience, **Arvato Financial Solutions** can create **Custom Consulting** experiences for customers in need. The portfolio includes project and change management, solution design, and **Advanced Analytics**. **Advanced Analytics** helps identify possible areas for change, utilizing machine learning, artificial intelligence technology

and platforms. In this framework, it is possible to recognize patterns, detect anomalies, and produce forecasts to generate recommendations for optimizing financial digital business processes and strategies. Industry insights, international revenue cycle management experience, and benchmarking all serve to support statistical methods and address a number of key performance indicators.

Arvato Financial Solutions' Fraud Management Consulting evaluates fraud models, provides insights and analytical knowledge across all industries. The fraud management is handled through an account team, which can offer process assessment and suggest areas for potential optimization.

Operational and Technical Consulting is also available through **Arvato Financial Solutions'** technical client management and integration team. Project setup, implementation, and process optimization services are offered. They follow up after the implementation phase to monitor and ensure sustainable, positive effects on business. This is often done prior to integration. Training is passed on in order to better handle technical needs in the future.



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.