The Revenue Optimization Solution Guide

Maximize revenue, mitigate risk

cybersource
A Visa Solution

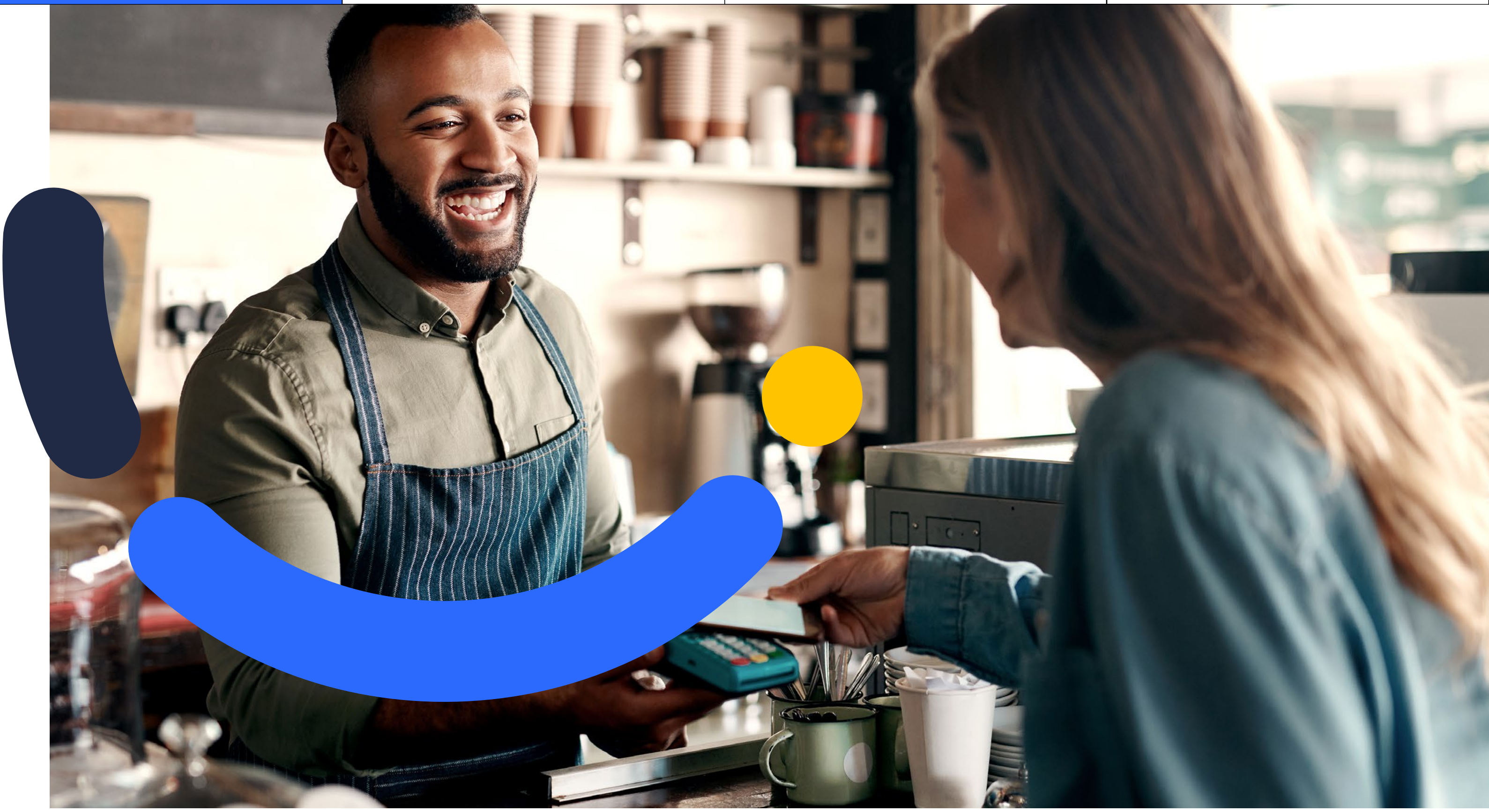
Content overview

Introduction

Approach

Solution

Get started



Introduction

Revenue Optimization Solution

Fraud management has come a long way from the early days of stopping fraud at any cost. Businesses have learned to balance the impact of fraud losses with operational costs and driving growth, while the pandemic spurred innovation in payment channels and changed customer behaviors.

Cybersource meets the moment with its fully automated Revenue Optimization Solution.

> “Businesses have learned to balance the impact of fraud losses with operational costs and driving growth.”

A historical perspective

What got us here won't get us there

In the early days of eCommerce fraud management, strategies were ruleset-driven and focused on deterring fraud. Built using lagging chargeback data, rules and models were often inaccurate and quickly outdated, leaving merchants vulnerable to placement on monitoring programs.

Merchants typically responded by rejecting higher volumes of orders based on moderate-to-high risk indicators or sent increased traffic to manual review, lowering efficiency, and driving up operational costs.

As eCommerce matured, merchants recognized fraud as a persistent threat that cannot be fully eliminated. At the same time, the availability of third-party data in fraud systems evolved, including key device fingerprint technologies as well as identity and data verification services.

Enhancements to systems and strategies allowed businesses to focus on cost management and improving the customer experience.

Fraud managers sought to optimize operations by striking the right balance between minimizing fraud losses, maximizing revenue, and controlling costs. In 2019, the Global Fraud and Payments Report[1] indicated that many businesses felt they had fraud losses under control and stabilized them at levels that minimized negative impacts on revenue and customer satisfaction.

The global pandemic has been a universal disruptor, accelerating the need for businesses to adopt innovative methods to serve their customers.

Merchants added mobile apps and chatbots, rolled out programs such as buy online, pickup in

[1] Source: 2019 Global Fraud Report; https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2019.pdf

store (BOPIS) and curbside pickup, added new payment methods such as buy now, pay later (BNPL) and third-party payments such as crypto, and adopted digital wallets. Customers responded in kind, changing their behaviors to leverage these new technologies while still expecting a frictionless experience.

Fraudsters also took advantage of innovation, executing attacks that blend in with changing customer behaviors. This came at a price: 33% of merchants report that they now struggle to identify and respond to emerging fraud attacks and 28% struggle with effectively using data to manage fraud, as stated in the 2022 Global Fraud and Payments Report.[2]

Increased fraud costs and KPIs—without a corresponding increase in revenue to manage fraud—has left many merchants prioritizing the reduction of fraud and chargebacks over improving the customer experience. Additionally, 60% of merchants reported in the 2022 Global Fraud and Payments report that they wish to reduce their reliance upon—or eliminate completely—the need for manual review.[2]

Merchants are seeking solutions to help them increase automated decisioning without incurring additional risk.

> “33% of merchants report that they now struggle to identify and respond to emerging fraud attacks.”

[2] Source: 2022 Global Fraud and Payments Report; https://www.cybersource.com/en/solutions/fraud-and-risk-management/fraud-report.html

Striking a new balance

A holistic approach to maximizing revenue acceptance

Fraud management is—and always will be—a critical component of business. The next phase of Cybersource's support of our merchants, however, extends beyond mitigating fraud risk to recapturing lost revenue by optimizing authorization conversions. In the 2022 Global Fraud and Payments Report, only 30% of merchants reported an awareness of their payment authorization rates.[2] Globally, issuers reject 18% of CNP traffic on average, compared with 3% of CP traffic.[3]

On the surface, the gap between CNP and CP authorization rates does not make much sense. eCommerce businesses own most of the liability for fraudulent CNP transactions, and a fraudulent transaction typically means a lost sale, a fine to the issuer, loss of revenue, and damage to the brand—including cart abandonment and lost loyalty.[3] Given these potential negatives, merchants have largely brought fraud under control, but this is not reflected in higher authorization rates. To close this gap, it is critical that all the players in the ecosystem work together.

Cybersource, as a wholly owned subsidiary of Visa and a pioneer in the payments industry, is poised to meet the moment, working closely with the broader Visa organization and issuers to strike a new balance with a common goal: To lead with acceptance, maximizing revenue while mitigating risk. Priorities include enhanced fraud management tools and analysis, greater visibility into authorization rates, and reduced processing friction.

[3] Source: Cybersource Revenue Capture whitepaper; https://www.cybersource.com/content/dam/documents/en/cybersource-revenue-capture-whitepaper-2020.pdf

Five key initiatives

To achieve this new balance, Cybersource is driving five key initiatives: lowering chargeback rates, increasing visibility to authorization rates in reporting, pre-screening fraud prior to authorization, optimizing tool configuration, and preserving the customer experience with automated authentication.

Lowering chargeback rates

This has been a key priority for eCommerce merchants for some time, but it becomes more pressing when one considers that authorization rates are tied to chargeback rates.[2] Merchants with higher chargeback rates are often distrusted by issuers, who may be less willing to accept traffic. Lowering chargeback rates may boost trust and ultimately authorization acceptance rates.

Visibility of authorization rates in reporting

As mentioned earlier, only 30% of merchants in the 2022 Global Fraud and Payments Report stated that they are aware of their authorization rates.[2] Understanding this metric helps the merchant establish a baseline and enables them to identify opportunities for improvement.

Pre-screening fraud prior to authorization

Many merchants now recognize that if fraud screening is moved upstream and prior to the authorization request, there is low-hanging fruit that may be eliminated. Card testing schemes, which were the top fraud trend observed for North American merchants in the 2022 Global Fraud and Payments Report, can be quickly identified and blocked using a pre-screening methodology, along with transaction events containing data with negative history that would otherwise be rejected post-authorization.[2] Removing these from traffic sent for authorization helps “clean up” and reduce the risky transactions observed by issuers, potentially reducing authorization decline rates.

Optimizing tool configurations

When a merchant pre-screens for risk prior to authorization, machine learning can be used to recommend further actions within the risk review process. For example, Cybersource's powerful machine learning model—backed by 141 billion transactions from VisaNet[4]—can be leveraged to determine if an event has either a positive or negative history; automated decisioning to accept or reject these events can be built into the strategy, reducing the pool of unknown or questionable characteristics subjected to further screening.

Preserving the customer experience with automated authentication

Cybersource has fully integrated 3DS capabilities into Decision Manager with Payer Authentication, enabling users to manage the customer experience with an end-to-end authorization flow and transparent transaction reviews.

The merchant can filter out clearly good and bad transactions up front and send the questionable transactions for authentication to reduce the need for manual review and optimize decisioning.

> "Cybersource Revenue Optimization Solution leads with automation and acceptance so that merchants can focus on growth."

Working together, this new balance helps ensure that merchants maximize revenue, issuers have better data that gives them confidence in approving good orders, and customers receive their products.

How is this accomplished? Powered by industry-leading machine learning and artificial intelligence, and curated by insights from an experienced global team, Cybersource Revenue Optimization Solution leads with automation and acceptance so that merchants can focus on growth.

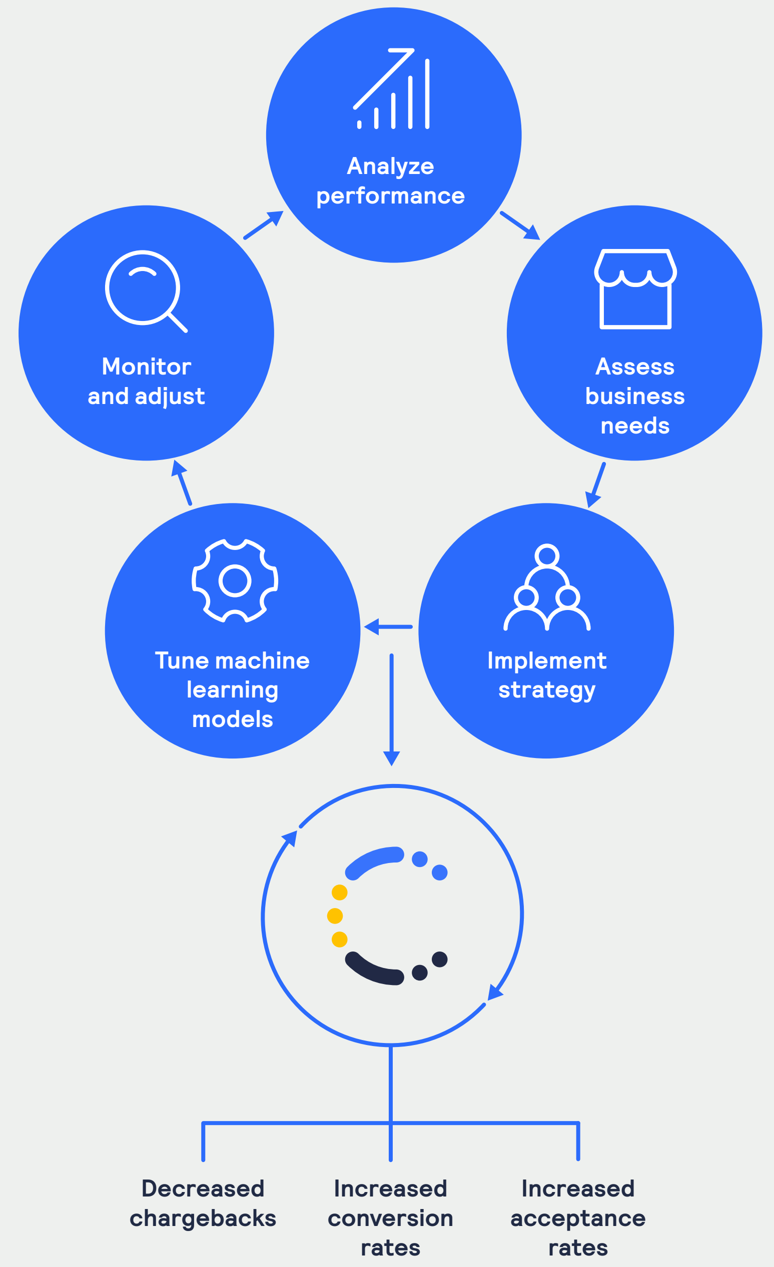
[4] Source: VisaNet transaction volume based on 2020 fiscal year. Volume may not include domestically routed transactions.

Revenue Optimization

Our Revenue Optimization Solution is all-inclusive and fully outsourced, allowing businesses to increase customer conversion and optimize revenue in real time with advanced automation, one of the largest data networks, and unparalleled expertise.

Cybersource offers the simplicity of a single, end-to-end platform that leverages machine learning and AI to automate risk management in a trusted fraud management tool that is easy to implement and fully integrated with device profiling, 3DS authentication capabilities, and third-party data services. Merchants report that they use at least four fraud products on average[2]; Revenue Optimization Solution is flexible, scalable, automated, and from a single connection and a single provider with the ability to share learnings across tools.

> "Revenue Optimization Solution is flexible, scalable, automated, and from a single connection and a single provider with the ability to share learnings across tools."



Our solution is focused on increasing acceptance rates and lowering chargebacks by understanding a merchant's unique use cases, implementing a strategy to maximize revenue, fine-tuning with industry-leading machine learning risk models, and adjusting as needed to reach optimization.

The how of revenue optimization

Each solution can be customized to the needs of each merchant, leveraging the expertise of a risk consultant specialized in Cybersource's risk management suite and analytics and aligned with each merchant's goals.

This solution is flexible enough to pivot strategies, test, and manage fraud as it evolves, avoiding costly IT resources, tickets, or additional related expenses. It scales to each merchant's growth, regardless of region or innovation, while maintaining the simplicity of a single agreement.

Decision Manager

Our flagship platform combines powerful machine learning and global merchant data to assess risk, while maintaining the flexibility to adjust in real-time for policy changes and emerging fraud patterns.

Payer Authentication

If an additional layer of protection is needed, we block fraudulent transactions before they're sent for authentication with 3DS to help reduce chargeback rates and manual reviews.

Email and identity verification data resources

Within Decision Manager, we include email and identity verification resources to enhance and increase the intelligence available for use in optimizing risk and acceptance strategies for authorization helps "clean up" and reduce the risky transactions observed by issuers, potentially reducing authorization decline rates.

Managed Risk Services

With nearly 70 consultants around the globe—and 750+ years of combined eCommerce experience—our risk consultants help ensure our customers find and maintain the right balance of maximum acceptance with risk mitigation.

Configurations may vary based on merchant needs.

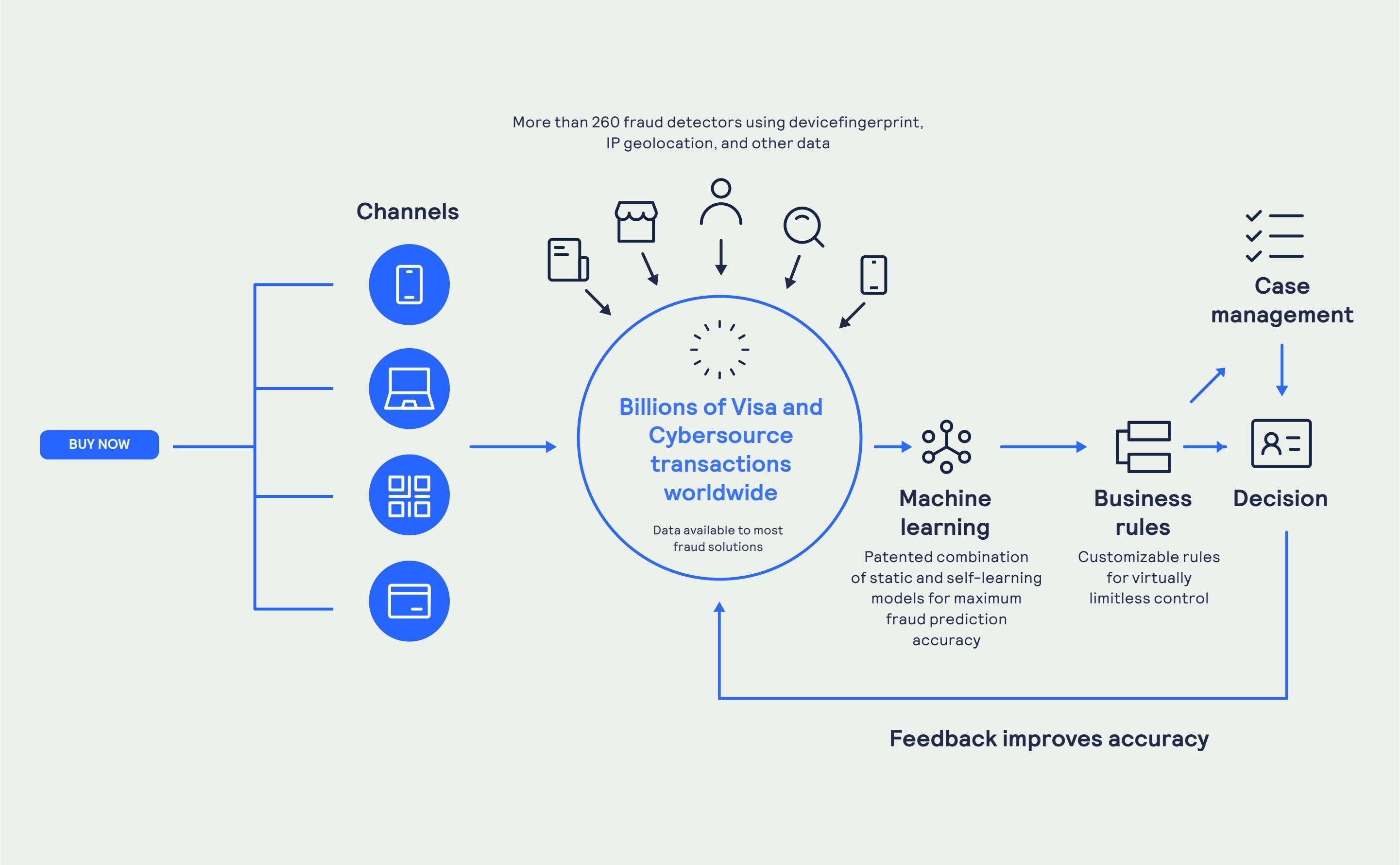
Decision Manager

Decision Manager is Cybersource's flagship fraud and risk management solution that allows businesses to accept or reject incoming orders based on a variety of sophisticated risk models. It is available fully integrated with Cybersource's payment management platform or as a standalone service.

> "Drives top-line growth as well as improved customer experience during the payment process."

Decision Manager has the flexibility to leverage machine learning and customized fraud rules to filter and reject high-risk transactions prior to submitting them to the issuer, which helps raise transaction conversion and could influence issuers to increase authorization rates. This drives top-line growth as well as improved customer experience during the payment process.

Decision Manager's advanced machine learning models help businesses evaluate their historical transaction data to find patterns, identify and implement new revenue optimization strategies, and make better payment decisions. Decision Manager provides powerful, flexible rules management capabilities that gives businesses the control they need to create precision rulesets that help reduce chargeback rates while being carefully attuned to their organization's broader sales and customer experience goals.


More than 260 fraud detectors using devicefingerprint, IP geolocation, and other data
Channels
BUY NOW
Billions of Visa and Cybersource transactions worldwide
Data available to most fraud solutions
Machine learning
Patented combination of static and self-learning models for maximum fraud prediction accuracy
Business rules
Customizable rules for virtually limitless control
Case management
Decision
Feedback improves accuracy

Key features and functionality:

- **Identity Behavior Analysis** captures insights from the broader global and merchant consortium, giving merchants the ability to easily recognize good and bad behaviors and automatically detect new customers. This accelerates fraud detection and promotes confidence around the acceptance of genuine and recurring transactions that boost bottom lines.

- **Decision Manager Replay** allows merchants to quantify fraud strategies in real time prior to activating in a live production environment. It is essentially a "what-if" testing function that retroactively applies a merchant's historical data to a new rule or strategy. The real-time reports show likely changes to review rate distribution and fraud rates, enabling the ability to pivot with confidence or plan and execute new strategy.

- **Rules Suggestion Engine** uses the outputs of Decision Manager's machine-learning models as inputs into the rule creation process. The Rules Suggestion Engine draws on a merchant's unique transaction history to present recommended rules that can augment existing fraud strategies. Each rule is accompanied by metrics to help merchants measure performance against the selected transaction data.

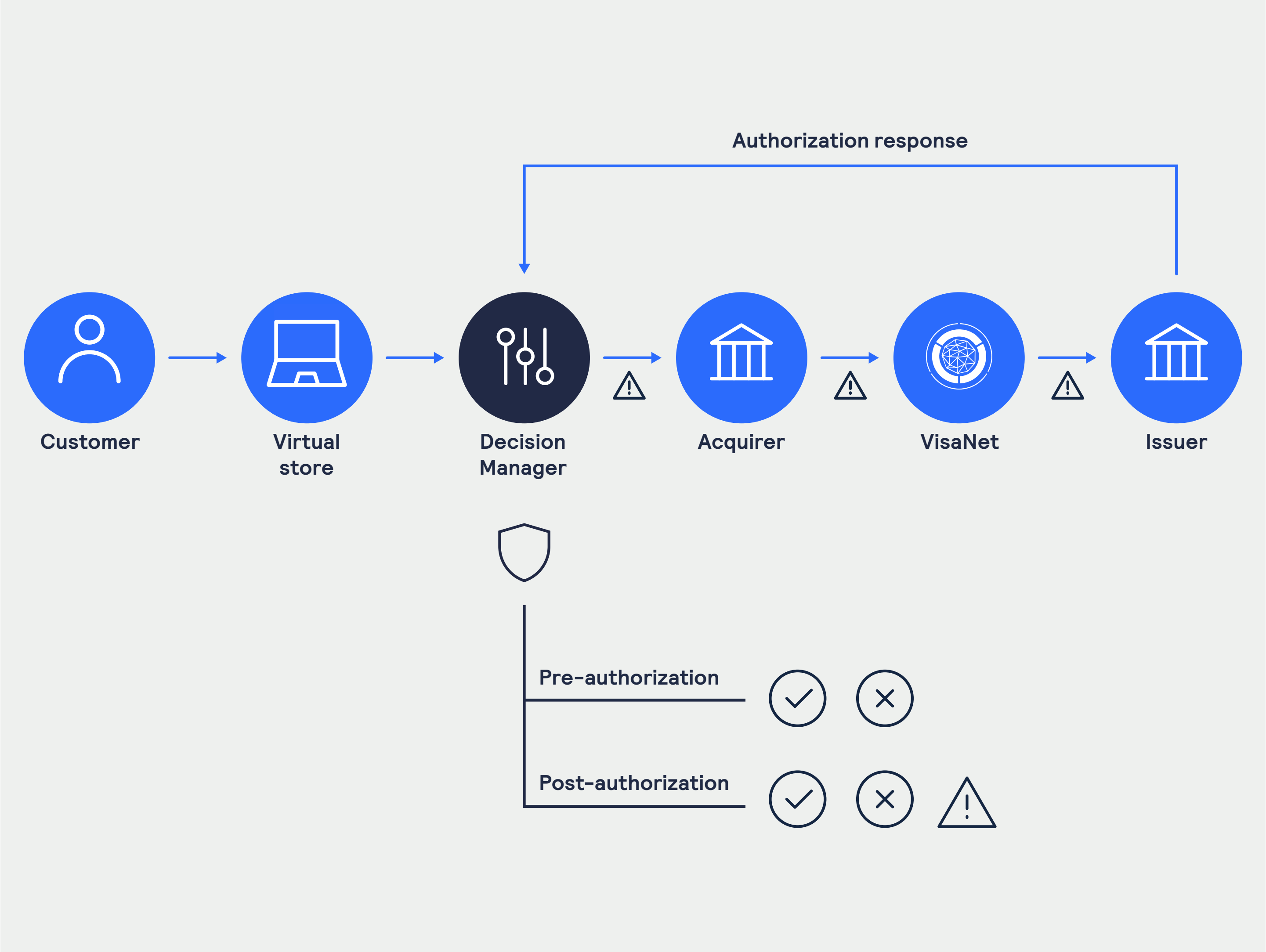
- **Third-party integrations** can be designed with rules to interact with multiple global validation services for enhanced authentication. Users can build multiple screening profiles based on product category, SKU, country, channel, and more. Default predictive models are available based on region and industry. This includes third-party validation services such as email and identity verification data resources.

Payer Authentication

Payer Authentication is Cybersource's 3-D Secure service that deters unauthorized payment card use and can help protect the merchant from fraudulent chargeback activity. Payer Authentication uses the EMV® 3-D Secure protocol for authentication and leverages the Cardinal MPI.

When Payer Authentication is used with Decision Manager, a merchant can optimize decision-making with Decision Manager's business rules to reject transactions before authorization if they are deemed too risky, invoke or suppress Payer Authentication based on order information, skip authentication if there is a potential impact on good customers, and use Payer Authentication results after authorization to reduce review rates.

> "Using Decision Manager plus Payer Authentication provides an additional layer of protection, enhances decision-making with extra insights, and gives merchants control of the customer experience."

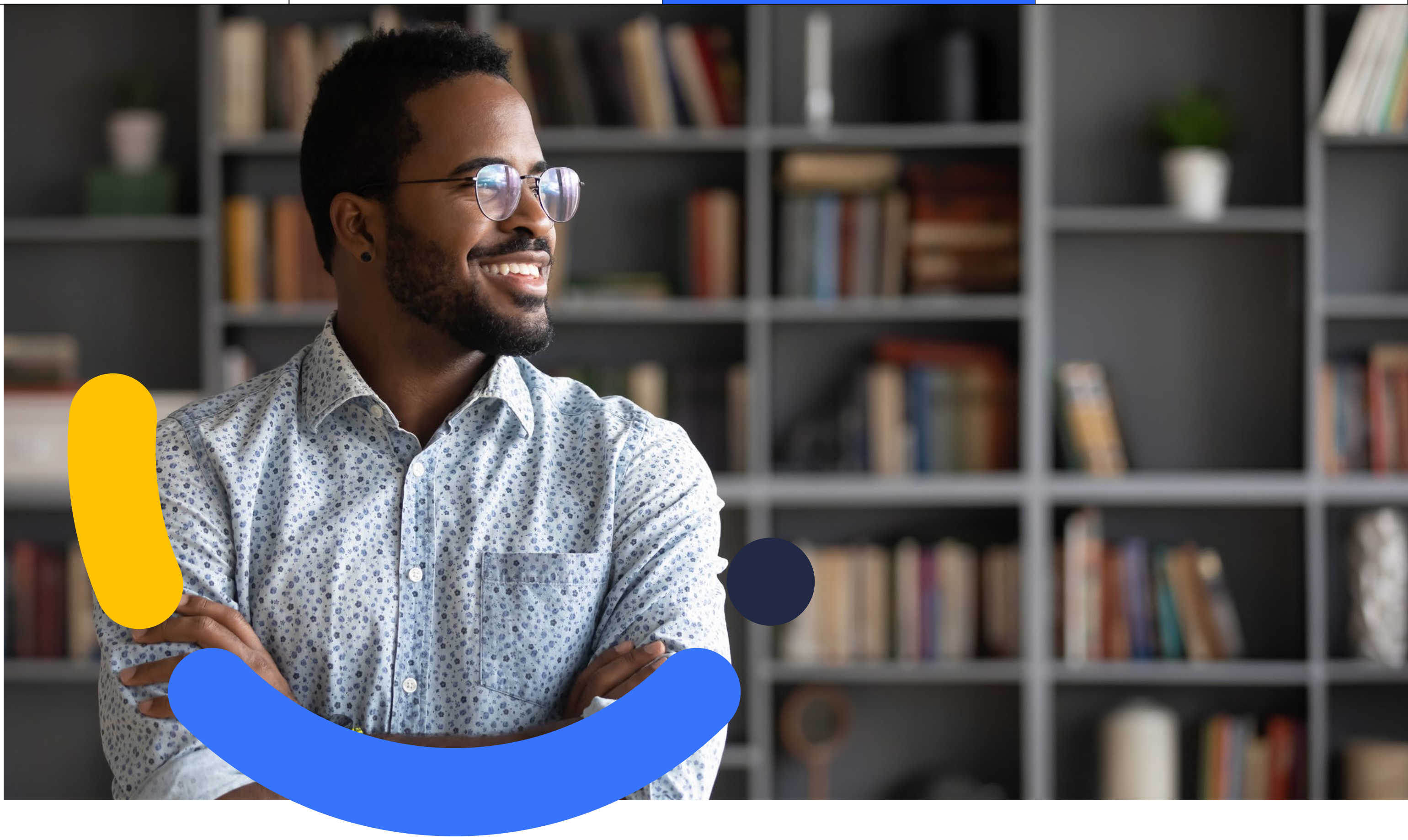


The benefits of Decision Manager and Payer Authentication are now available in one risk management tool. Using Decision Manager plus Payer Authentication provides an additional layer of protection, enhances decision-making with extra insights, and gives merchants control of the customer experience.

- Shift liability for fraudulent transactions back to issuers. When you use Payer Authentication on qualified transactions, the issuing bank becomes liable for any fraud-related chargebacks on those transactions.

- Reduce chargeback rates by attempting to block fraudulent transactions before they're sent for authorization. This helps catch potentially problematic transactions before they have a chance to result in fraudulent chargebacks.

- Lift authorization rates by filtering out more bad transactions and sending higher quality transactions through for authorization, providing issuers with the additional information to make better risk assessments and approve more transactions.



Managed Risk Services

Performance monitoring is at the heart of the Revenue Optimization Solution, driving the customization of a merchant's strategy with an expert in Decision Manager, Payer Authentication, applying identity and email verification services, and using analytics and insights serving as a trusted resource. Managed Risk Analysts are seasoned fraud professionals and risk consultants, experienced in use cases across the globe and in every vertical.

Key benefits

- Provides performance monitoring
- Performs analysis that generates insights
- Evolves fraud strategy
- Utilizes specialized fraud products
- Applies identity and email insights
- Understands the changing fraud landscape
- Serves as a trusted fraud resource

Fraud managers today are expected to wear many hats, including operations, marketing, logistics, payments, disputes, and customer service—and are often considered the "gatekeeper" to future growth. These expanded roles and responsibilities have left many merchants feeling that they cannot keep up with emerging fraud trends and support the day-to-day; outsourcing this function to Cybersource allows merchants to focus on business needs while a trusted professional turns the dials.

Proven results
Businesses that optimized their acceptance strategies with Cybersource [5]:

- Saved $4 million in manual review costs and increased acceptance by $36.8 million in 2021.
- Saw an 8% increase in acceptance rates on average.
- Saw a 1% increase in authorization rates on average.

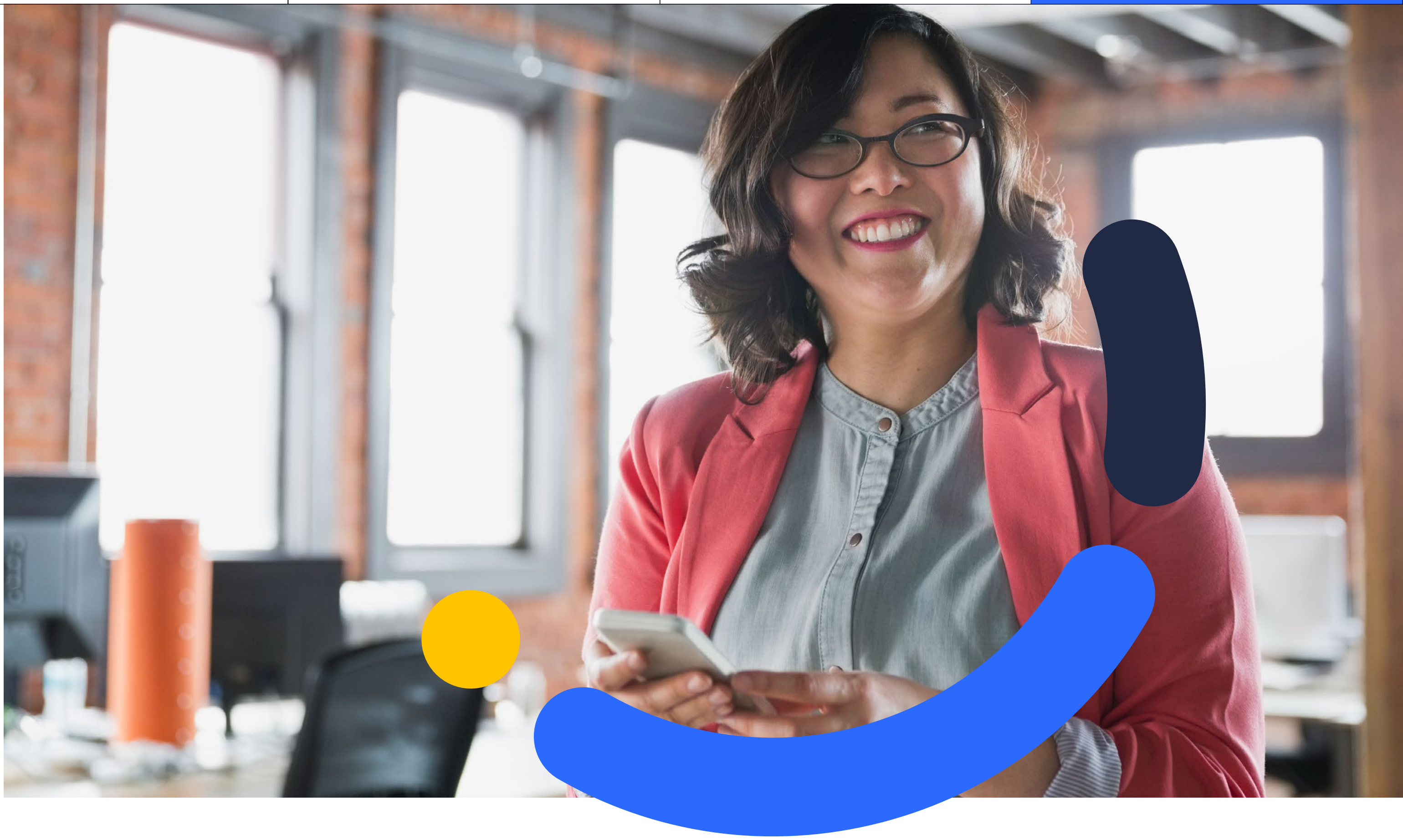
Optimize revenue while managing payment fraud

Powered by industry-leading machine learning and artificial intelligence, and curated by insights from a tenured global team, Cybersource Revenue Optimization Solution leads with automation and acceptance so that merchants can focus on growth.

www.cybersource.com

For an in-depth industry view,
learn more in the
2022 Global Fraud and Payments Report.

[5] Required Disclosures: Results calculated using internal data based on Decision Manager clients in North America during January 2020 to November 2021. Results will vary based on factors including if client works with Cybersource Managed Risk



About Cybersource

At Cybersource, we believe that agility is the key to success in today's fast-changing world. We help you create and evolve payment solutions your way, so you can stay ahead.

Your customer is more than a transaction and Cybersource Token Management Service elevates your tokenization strategy from a basic payment security tool into a complete, 360-degree view of every customer, helping you deliver the great experiences you've always wanted.

Join the thousands of businesses that already depend on Cybersource Token Management Service to keep payments simple and secure—so payment complexity never gets in the way of better experiences and more good business.

Contact us to chat with a Cybersource representative or to request an appointment.

Citations

[1] **Source:**
2019 Global Fraud Report;
https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2019.pdf

[2] **Source:**
2022 Global Fraud and Payments Report;
https://www.cybersource.com/en/solutions/fraud-and-risk-management/fraud-report.html

[3] **Source:**
Cybersource Revenue Capture whitepaper;
https://www.cybersource.com/content/dam/documents/en/cybersource-revenue-capture-whitepaper-2020.pdf

[4] **Source:**
VisaNet transaction volume based on 2020 fiscal year. Volume may not include domestically routed transactions.

[5] **Required Disclosures:**
Results calculated using internal data based on Decision Manager clients in North America during January 2020 to November 2021. Results will vary based on factors, including if client works with Cybersource Managed Risk.