Revenue Capture

The next generation of eCommerce payments and fraud management

cybersource
A Visa Solution

Table of contents

Founded in 1994, Cybersource was one of the world's first eCommerce payment management companies. One of the pioneers in online payments processing and fraud management for medium and enterprise businesses for over two decades, Cybersource offers a complete portfolio of eCommerce payment solutions. In 2010, Cybersource became a wholly owned subsidiary of Visa, Inc. Today over 450,000 businesses around the world trust Cybersource to streamline their online payment solutions.[1]

[1] As of 06/02/2020. Includes Authorize.Net businesses.

The Next Frontier in Fraud: Working With Issuers to Improve Authorization Rates

eCommerce revenue is currently doubling approximately every 4.5 years,[2] but capitalizing on that growth requires a nuanced approach to managing eCommerce transactions that helps issuers accept more authorization requests with greater confidence.

[2] Assuming average eCommerce growth rate of 15% continues; uses YOY % growth rates 2010–2019 found in "US ecommerce sales grow 14.9% in 2019", Digital Commerce 360. Available: https://www.digitalcommerce360.com/article/us-ecommerce-sales/. These estimates do not take into account any impacts to eCommerce caused by the COVID-19 pandemic.

Fraud Management:
A Historical Perspective

To fully understand Cybersource's Revenue Capture initiative, it's important to first examine how fraud management strategies have changed over time.

As Figure 1 shows, fraud management strategies have evolved significantly over the last decade, growing from a set of rules that focused almost exclusively on deterring fraud, regardless of the costs (Fraud 1.0); to a more nuanced approach, centered around balancing accuracy, operational efficiency and customer experience (Fraud 2.0); to the most recent development — a strategic initiative from Cybersource designed to help businesses recover revenue lost to card-not-present issuer declines (Fraud 3.0).

Fraud 1.0

Stop fraud now!
10 years ago

Fraud 2.0

A better balance
5 years ago

Fraud 3.0

Revenue Capture
Present

Figure 1 | The evolution of fraud management strategies. Cybersource 2020.

Fraud 1.0

The early fraud prevention engines were built using chargeback data — typically reported at a delay of up to 30 days, sometimes longer — which meant their fraud strategies or models were often inaccurate and quickly outdated. As a result, some organizations were hurt by high chargeback rates or placed on monitoring programs.

Subsequently, many of those businesses elected to automatically reject higher volumes of orders based on high-risk and even moderate-risk indicators. But this sole focus on minimizing fraud led to increased rejections of legitimate orders due to suspicion of fraud (known as "false positives"), resulting in lost revenue and a poor customer experience. Correspondingly, businesses that focused on increasing acceptance to improve the customer experience in the face of a fraud threat wound up sending more transactions to manual review — resulting in lower efficiency and increased operational costs.

Businesses faced a difficult dilemma: there were no easy solutions for how to manage fraud effectively; fraud costs, customer satisfaction and operational costs were inextricably linked. Pushing any one of these levers impacted the other two.

> In the early days of fraud management, businesses were purely reactive. Stopping fraud was the primary objective.

Fraud 2.0

The next evolution in fraud management came about when businesses realized that fraud had become a persistent threat and they couldn't tackle these issues individually; they had to confront all three simultaneously. As seen in Figure 2 below, the challenge now was to find a way to optimize their operations by striking the right balance between minimizing fraud losses, maximizing revenue and controlling operational costs.

The second phase of fraud management strategies required teams to optimize their operations by finding the minimum combination of all three costs.

Fraud management teams had to hire more employees to handle the increases in manual reviews. Additionally, many businesses were spending a significant amount of money developing internal fraud solutions as they came to terms with fraud. These growing operational costs also led many businesses to re-evaluate their understanding of fraud management.

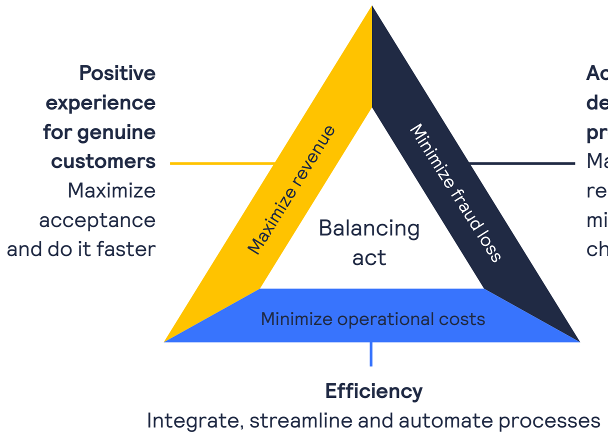

Positive experience for genuine customers
Maximize acceptance and do it faster
Maximize revenue
Balancing act
Minimize fraud loss
Accurate fraud detection and prevention
Maximize rejection, minimize chargebacks
Minimize operational costs
Efficiency
Integrate, streamline and automate processes

Figure 2 | The fraud management balancing act. Cybersource 2020.

Fraud costs are dynamic by nature, and with several years of accumulated fraud management experience under their belts, many businesses now had enough fraud management experience to understand how these three costs interacted with one another.

During this second phase, systems and strategies matured, allowing businesses to focus their attention on more realistic cost management and improving their customer experience. Device fingerprinting and third-party data verification became more ubiquitous, making it easier to directly pinpoint malicious users and organized fraud rings. Businesses became better at identifying and rejecting truly high-risk transactions before the manual review process, reducing the operational burden imposed by manual reviews.

A New Era for eCommerce

In "Masters of Balance: What it takes to be a fraud management leader," Cybersource's 2019 Global eCommerce Fraud Management Report, many businesses reported they brought their fraud losses largely under control and stabilized them at levels that minimize negative impacts to revenue or customer satisfaction.[3]

Fraud 3.0

Fraud management will always be an extremely important part of any organization's eCommerce strategy — however, most businesses (particularly mature ones) have already found their unique fraud balancing point.

Cybersource's Revenue Capture initiative marks the beginning of a new era. As an industry leader in payments and fraud management, we are teaming up with other Visa businesses and collaborating with issuers and acquirers where we have fostered working relationships. Because the next step in fraud management extends far beyond fraud management — it's actually about recapturing lost revenue by optimizing authorization conversions.

Figure 3 | Cybersource Vice President of Risk Solutions, Andrew Naumann, explains how Cybersource is collaborating with issuers and businesses to increase eCommerce authorization rates in the Revenue Capture video, available here. Cybersource 2020.

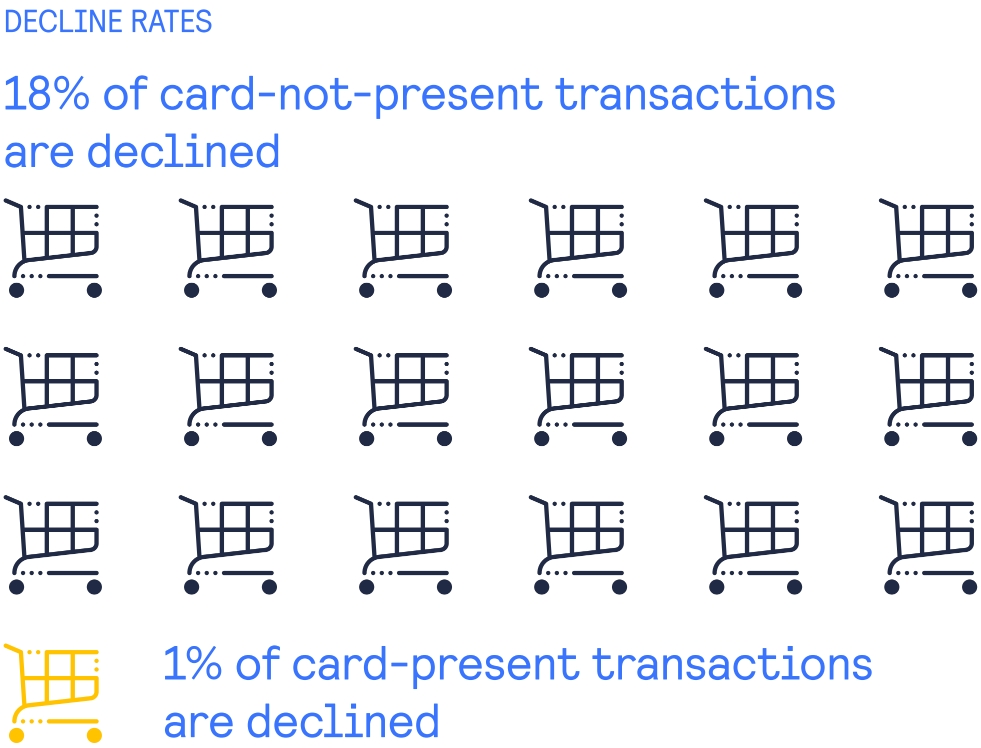
[3] Question: Please indicate your order rejection rate for percentage of orders rejected due to suspicion of fraud. Possible answers: 1. [ ]% 2. Don't know 3. Don't track. "Masters of Balance: What it takes to be a fraud management leader," 2019 Global eCommerce Fraud Management Report, Cybersource.

So what's next?

Potential eCommerce revenue growth is huge. eCommerce sales are expected to grow at up to five times the rate of brick-and-mortar sales through 2023.[4] If current growth rates continue, eCommerce will likely exceed $5.5 trillion in sales in the next few years.[5] Maximizing revenue growth from this channel is critical, and the best way to do this is by closing the gap between card-not-present (CNP) and card-present (CP) authorization rates to help businesses potentially recapture billions in lost revenue each year.

Cybersource's Vice President of Risk Solutions, Andrew Naumann, and other fraud management experts at Cybersource are now working with issuers to improve their CNP decline rates, which currently sit at around 18% — far higher than their 1% decline rates for CP transactions.[6]

This authorization gap equates to potentially billions in lost revenue each year in the U.S. alone.[7]


DECLINE RATES

18% of card-not-present transactions are declined

1% of card-present transactions are declined

Figure 4 | The eCommerce authorization gap. Cybersource 2020.

[4] eMarketer, Worldwide Ecommerce Retail Sales, May 2019
[5] Assuming average eCommerce growth rate of 15% continues; uses YOY % growth rates 2010-2019 found in "US ecommerce sales grow 14.9% in 2019", Digital Commerce 360. Available: https://www.digitalcommerce360.com/article/us-ecommerce-sales/. These estimates do not take into account any impacts to eCommerce caused by the COVID-19 pandemic.
[6] VisaNet, Authorization rates in the United States in Q4 2018
[7] Cybersource calculations based on eMarketer and VisaNet data

Closing the card-not-present authorization gap requires a groundbreaking approach that Cybersource has the scale and experience to deliver.

The Card-Not-Present Authorization Gap

eCommerce has a trust issue.

Though fraud rates have grown a small amount over the last few years, the medium-term average percentage of revenue lost to eCommerce fraud has remained relatively stable. This stability suggests businesses have found their ideal equilibrium points for managing CNP fraud costs.

However, issuers are still declining CNP transactions at disproportionately higher rates. As far as they are concerned, CNP transactions still lack the level of validating data that are available during CP transactions, which means CNP transactions in the absence of validating data appear far riskier to issuers than they do to businesses. Consequently, issuers are far more likely to reject CNP transactions than businesses — declining 18% of all eCommerce transactions, as noted above. Compare that to the results from the 2019 Cybersource Global eCommerce Fraud Management Report, in which respondents reported declining an average of just 3% of CNP orders due to high risk scores.[8]

But why does the authorization gap exist in the first place? eCommerce businesses own most of the liability for fraudulent CNP transactions, with very little falling on the issuers. If a transaction turns out to be fraudulent, the business not only loses that sale, they must also pay a chargeback fee to the issuer. These CNP businesses not only bear the brunt of a far greater impact on their revenue when issuers reject a transaction too aggressively, they also face increased cart abandonment rates and the loss of loyal customers to competitors.

Issuer Declines Can Create Hidden Problems

When legitimate orders get rejected by the issuer, businesses may:

- Lose a sale
- Send a customer to a competitor
- Overwhelm Customer Service teams
- Risk negative word of mouth

Figure 5 | Possible negative impacts of issuer declines. Cybersource 2020.

[8] % of eCommerce orders declined after manual review (Global): 3%. P. 32, "Masters of Balance: What it takes to be a fraud management leader," 2019 Global eCommerce Fraud Management Report, Cybersource.

With the direct incentives falling on them, it should come as no surprise that most eCommerce businesses have brought fraud largely under control. More businesses are now running fraud solutions prior to authorization and they have more sophisticated fraud tools and strategies at their disposal than ever before — they can see more transaction insights than they could in the past and they have the levers in place to reject bad transactions more accurately — giving them greater confidence to approve more orders. As a result, the transactions that businesses confirm and send on to issuers — asking for payment authorization — are generally much safer to accept than issuers realize.

So why are issuers still rejecting so many of these transactions after businesses have approved them? Because many issuers are still solely focused on stopping fraud, but they are rejecting orders based on limited data points. Issuers don't have ready access to the new transaction data businesses are using, and they are not necessarily fully aware of how accurate and effective businesses' fraud management tools and decision-making strategies have become.

Businesses decline just 3% of CNP transactions.[9]

It is likely that some percentage of this group of rejected transactions are actually false positives; that is, legitimate orders by real customers that were incorrectly identified as fraudulent. Even though businesses continue working to improve detection accuracy to further eliminate false positives, there are still some customers who are negatively impacted. It's clear that no fraud solution is perfect; despite utilizing robust fraud management strategies, many businesses are still seeing an average 0.7% chargeback rate.[10]

[9] % of eCommerce orders declined after manual review (Global): 3%. P. 32, Cybersource, Ibid.

[10] Fraud coded chargeback rate, as a % of annual eCommerce revenue (North America, Middle East and Africa, Europe): 0.7%. P. 32, Cybersource, Ibid.

From this perspective, the issuers' divergent approach to managing fraud between the CP and CNP channels is understandable; CP transactions offer a dynamically generated identifier from an EMV chip, as well as face-to-face interaction with the cardholder, a signature and other identifying data points that help give issuers greater confidence in those transactions. By comparison, as far as issuers are concerned, CNP transactions appear far more anonymous — and malicious actors can use a number of strategies to circumvent risk signals. So, there is some risk, just not as much as issuers tend to expect.

As seen in Figure 4, even discounting for credit worthiness issues, the 18% of CNP transactions that get rejected annually likely amounts to billions of dollars in lost sales in the U.S. alone — an amount which will only continue to grow as eCommerce markets expand globally.[11]

It's important to note that issuers are evaluating transactions independently from the merchants and they have different criteria that impact authorization decisions. And of course, decline rates vary by issuer, vertical and region. Still, these declines amount to significant lost revenue, and it is critical that all the players in the payments ecosystem work together to move this number as close as possible to the business decline rate of 3%.[12]

Not to mention the impact these declines can have on customers. The loss of a good customer is extremely expensive. In today's competitive environment, consumers whose transactions are unceremoniously declined are most likely just one click away from switching to a competing business — not only for that particular transaction, but also for the balance of their lifetime ordering from that business.

The roles of fraud manager and payments manager are beginning to merge slightly as issuer declines are being essentially seen as external false positives. However, unlike internal false positives, the options to address this problem are limited.

That's where Revenue Capture comes in...

Card-not-Present data points

- ID verification missing
- EMV code missing
- Signature missing

Card-Present data points

- The card is physically present
- Identity can be verified with another form of ID
- EMV chip generates unique transaction code
- Signature can be obtained for verification at a later stage

Figure 6 | Issuers see limited data on card-not-present transactions compared to card-present transactions. Cybersource 2020.

[11] Cybersource calculations based on eMarketer and VisaNet data.

[12] % of eCommerce orders declined after manual review (Global): 3%. P. 32, "Masters of Balance: What it takes to be a fraud management leader," 2019 Global eCommerce Fraud Management Report, Cybersource.

The Five Initiatives of Revenue Capture
Building the Future of Fraud Management

Cybersource's strategies for recapturing lost revenue hinge on the fact that most eCommerce businesses have brought their fraud rates under control.

Thanks to our long history as one of the pioneers of eCommerce payments — and as a wholly owned subsidiary of Visa — Cybersource is uniquely positioned to help increase CNP authorization rates by fundamentally shifting the way businesses and issuing banks interact… and changing the way payments are processed.

To turn our Revenue Capture vision into reality, Cybersource fraud management and payments experts developed five key initiatives to help businesses take the next step in eCommerce top-line growth. Enhanced fraud management tools and analytics, greater visibility into authorization rates and reduced processing friction mean businesses get the revenue, issuers get the processing fee and buyers get their products.

1. Lowering Chargeback Rates

Issuer authorization rates are tied to a business's chargeback rates. If the business has a high fraud rate, issuers will be wary of authorizing their transactions. When a business lowers their chargeback rates, they are effectively signaling to issuers that they have improved their fraud management processes. Issuers correspondingly treat that business's transactions with a lighter touch, improving the business's authorization rate.

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

2. Authorization Rate Reporting

Fraud teams are typically immersed in data. Transaction information drives many decisions, from rule enhancements to manual reviews to determining whether or not to represent a chargeback. However, many fraud managers are currently in the dark regarding their issuer authorization status. Many businesses either didn't realize there was a problem or didn't think they had the power to drive change outside of their organizations.

Without an initial baseline, it's almost impossible for businesses to determine if they have an outsized authorization decline problem in the first place or effectively measure whether they are making progress to close the gap. Cybersource's first step is to help businesses see and understand their issuer authorization rates. In addition to tracking against past internal performance, Cybersource is helping businesses benchmark their performance against other organizations in similar industries and verticals.

Issuer Decline Next Steps

Businesses should develop deep institutional knowledge and protocols around these key points

- Know their decline rate
- Analyze the reasons why transactions get declined
- Review declines that occur after manual review; reevaluate tools and processes as needed
- Analyze declines from authorization reason codes; look for spikes and other anomalies

3. Pre-Screening Transactions Prior to Authorization

Businesses are increasingly recognizing the value of moving most or all of their fraud screening upstream, prior to the authorization request.

Changing the order of operations to submit transactions to Decision Manager prior to authorization may result in a slight increase in transactional fees, but the downstream advantages could be far more significant. Decision Manager's pre-screening process uses machine learning and the business's own fraud rules to clean up transactions prior to submitting to the issuer, which helps promote higher transaction conversion.

This approach allows businesses to filter and reject extremely high-risk transactions, or those originating with known fraudulent data points, prior to authorization submission — resulting in a cleaner set of transactions sent to the issuer.

These cleaned up transactions help reduce issuers' decline rates and operational burdens and they help drive improvements to the business's historical fraud rates. Over time, issuers will gain greater confidence in the business — resulting in an increased authorization acceptance. Improving authorization rates to recapture lost revenue is the end goal, and the impact on top-line growth will likely outweigh any increase in operational costs.

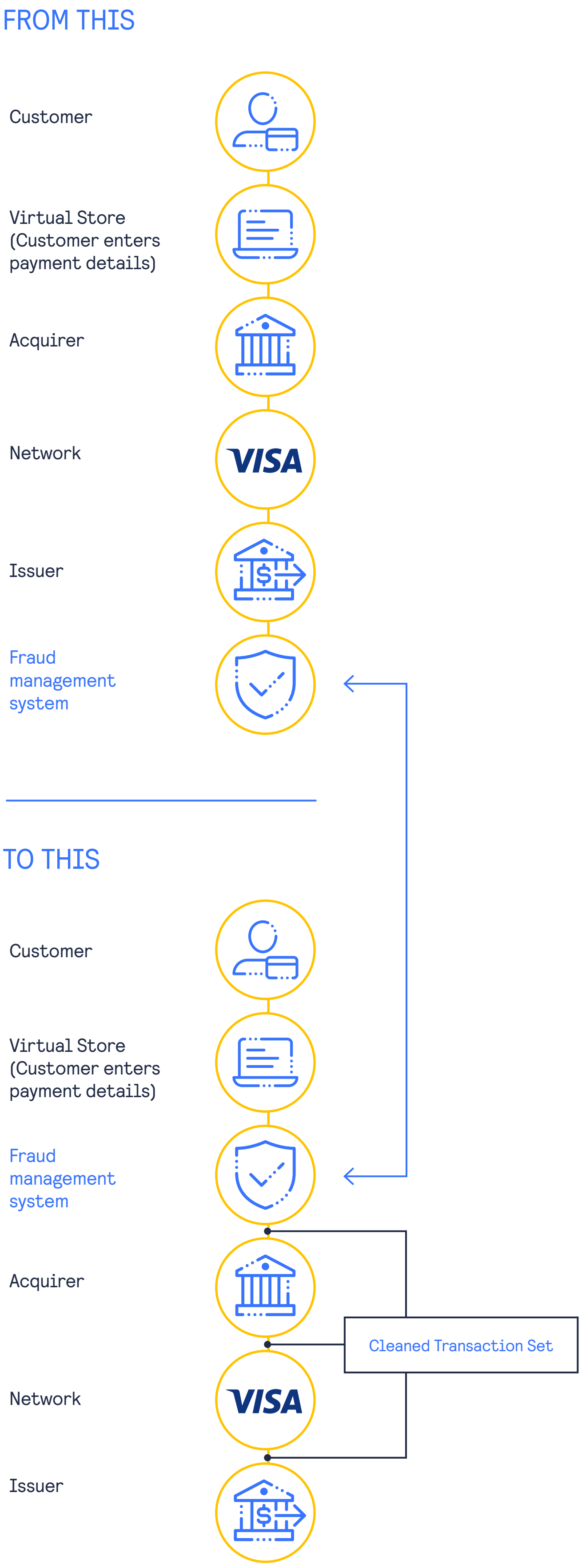


Figure 7 | Moving fraud screening upstream to provide issuers with additional information alongside authorization requests. Cybersource 2020.

Looking Back at Historical Fraud Transaction Strategies

Traditionally, businesses submitted their transactions to the issuing bank first, before submitting them for fraud screening, to ensure the accounts were active and funds were available.

This made sense for two reasons:

First, it gave businesses access to results from issuer response tools like Address Verification Services and Card Verification Number, which often enhanced the decision-making process.

Second, it helped mitigate operational costs by reducing transaction volumes before submitting them to a third-party fraud solution for evaluation.

4. Optimizing Tool Configurations

Organizations have a number of tools at their disposal: manual review, second-level processing, authentication and smart routing. How does one know which lever to pull and when — and what should be the appropriate sequencing of those tools? Decision Manager's leading analytics and reporting help optimize these tools, enabling Cybersource to create self-tuning feedback loops.

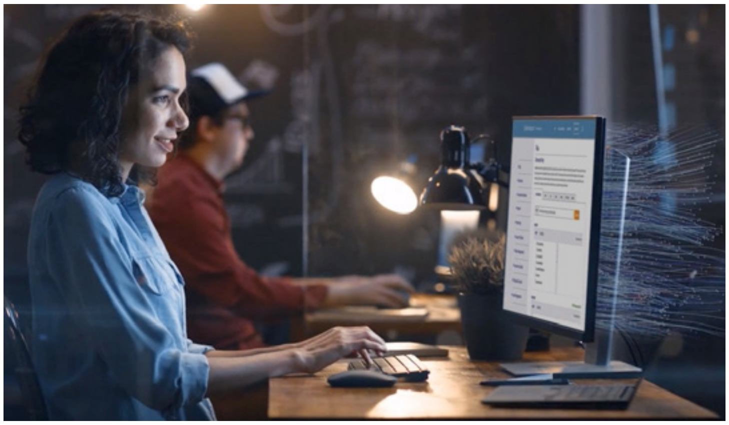


Figure 8 | Cybersource's Decision Manager uses machine learning to continuously improve its fraud-fighting capabilities. Cybersource 2020.

By using machine learning to orchestrate automatic rule calibration for operations like payment acceptance processing and transaction routing, Cybersource's Decision Manager reduces the decisioning load placed on fraud management teams — allowing them to better concentrate on the cases that get routed to manual review.

Continuously incorporating new transactional history and analyses of various decisioning permutations will optimize tool configurations and help maximize completion rates.

5. Preserving the Customer Experience with Automated Authentication

Cybersource is working with clients impacted by the European Union's second Payment Services Directive (PSD2) mandate for Strong Customer Authentication (SCA). Cybersource's Payer Authentication solution will help automate authentication and maximize exemptions to the PSD2 SCA mandate in order to reduce friction for customers during the payment process.

Payer Authentication, available through Decision Manager, gives businesses greater control over their customer payment experience, while also providing all the benefits of the latest generation of Cybersource's EMV® 3-D Secure solution[13] (which supports the requirements of SCA), including fraud liability shift and reduced interchange fees.

Implementing this tool allows businesses to decide when to request payer authentication protection — helping ensure a seamless checkout experience for their good customers and supporting compliance with the recent PSD2 SCA mandate requirements.

A combination of Cybersource's Payer Authentication solution, a robust fraud screening strategy and exemption optimization services will be necessary to keep authorization rates from dropping.

[13] EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

An Introduction to Strong Customer Authentication

The EU's PSD2 SCA mandate requires strong customer authentication on certain eCommerce payment transactions where both acquirer and issuer are in the European Economic Area, UK or Gibraltar. The directive's SCA mandate came into effect on Sept 14, 2019, while the enforcement is expected to start in 2021.[14]

When SCA is required, the payer is required to authenticate through at least two factors, each of which must be from a different category:

- ✓ **Something the payer knows** — PIN, Password, etc.
- ✓ **Something the payer has** — token generator, pre-registered mobile device, etc.
- ✓ **Something the payer is** — thumbprint, voice match, etc.

To learn more about PSD2, visit:
www.Cybersource.com/psd2

To learn more about SCA, visit:
www.Cybersource.com/en-gb/psd2-sca

eCommerce businesses who sell in this area need to be able to support SCA or they may see an increase in declined transactions.

Benefits of SCA

1. SCA delivers greater peace-of-mind for cardholders.
    a. Increased security measures, such as the ability for issuers to authenticate cardholder using two-factor authentication, will increase cardholder confidence when auth is successful.
2. SCA is a driver for innovation.
    a. SCA helped lead to the introduction of EMV 3DS 2 protocols. Compared to 3DS 1, EMV 3DS 2 protocols enable businesses to share 10x more data with issuers, enhancing issuers' authentication strategies and decision making.

[14] EBA Opinion, published October 16, 2019. Available: https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment

Future Innovations

Revenue Capture will continue evolving to find new ways to help close the CNP authorization gap. This section explores some future capabilities we have targeted for the next phase of development.

1. Intelligent Routing Tools

Intelligent payment routing processes will help businesses further boost authorization acceptance by analyzing historical transaction criteria to match different types of transactions with the appropriate acquirer in order maximize authorization rates.

Among other criteria, this functionality will take into consideration dollar amount and whether it's a cross-border transaction, as well as the actual card issuer, then route to the appropriate processor on the back end.

In the future, Decision Manager will be able to support API-based smart routing and will have the ability to configure rules on any API field in order to have the transaction routed appropriately. The capability to route transactions based on aggregated parameters (dollar amount, volume, etc.) will also be made available through Decision Manager as well.

CONFIGURABLE FOR INDIVIDUAL ORDERS

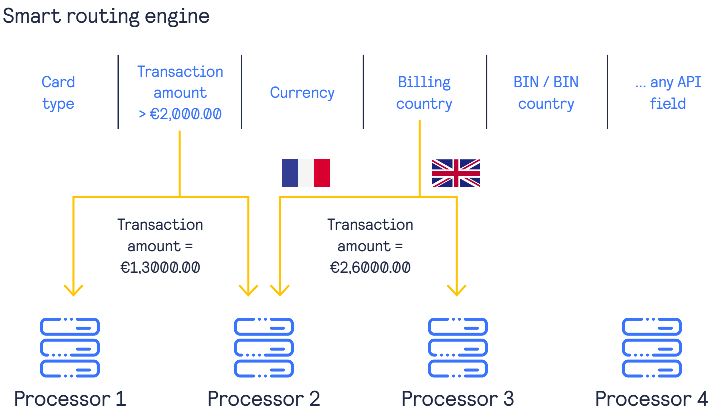


Figure 9 | Configurable for individual orders. Cybersource 2020

Intelligent payment routing can take into consideration amount, cross-border billing, card issuer, any API field and various aggregate parameters — then route transactions to the appropriate processor on the back end.

AGGREGATED FOR VOLUME OR AMOUNT

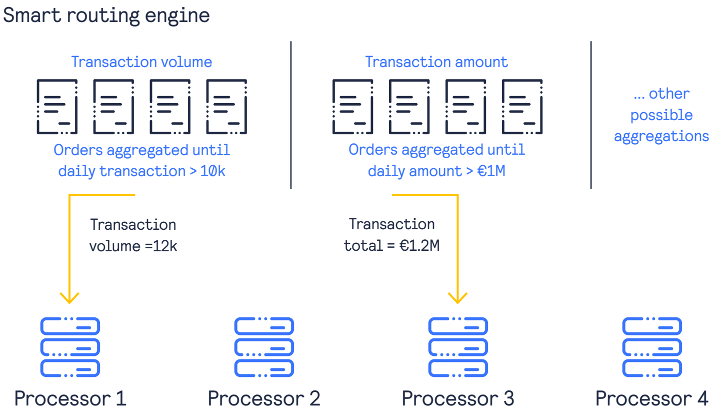

Smart routing engine
Transaction volume
Orders aggregated until daily transaction > 10k
Transaction amount
Orders aggregated until daily amount > €1M
... other possible aggregations
Transaction volume =12k
Transaction total = €1.2M
Processor 1
Processor 2
Processor 3
Processor 4

Figure 10 | Configurable for individual orders. Cybersource 2020

2. Chargeback Management with Verifi

Cybersource will be integrating Verifi's Order Insight into Decision Manager. Order Insight provides enhanced order data to issuers and customers at the first point of customer inquiry in order to help prevent disputes. Order Insight saves time for issuers, reduces confusion for customers and helps businesses reduce disputes and chargebacks, which also helps prevent brand damage and loss of customers. Most importantly, it converts what would have been a chargeback to a legitimate transaction.

3. Sharing Risk Scores with Issuers Prior to Authorization

Flipping the traditional script by running fraud rules prior to authorization in order to pre-screen transactions allows issuers to be more confident when accepting authorization requests. But we are also working on new capabilities that will allow businesses to share some of this pre-screening outcome data (e.g., risk scores, etc.) alongside the authorization request, in order to supplement issuers risk evaluations. Once a transaction request is able to include these additional data points, that will signal "this transaction has been pre-screened by Decision Manager," letting issuers know that these flagged transactions pose less risk.

Building Better Visibility and Greater Trust With Revenue Capture

With effective fraud strategies in place across most of the eCommerce marketplace and fraud losses holding stable at a lower, optimized percentage, businesses may finally be able to focus their efforts on maximizing top-line growth with Revenue Capture. The Fraud 3.0 era will be centered around reducing authorization declines, increasing visibility and building a better understanding of card-not-present transactions before authorization.

Cybersource is working with Visa, businesses, issuers and acquirers to build better, more-comprehensive communications between payment entities to increase visibility into CNP transactions and reduce decisioning friction and overall risk for all parties.

The most basic goals of Cybersource's Revenue Capture initiative are to increase issuer authorization rates, improve customer satisfaction and recover lost revenue. Only Cybersource and Visa have the experience, scale and connections to pioneer a change of this scope. Cybersource is proud to be an industry leader for payments and fraud management.

This whitepaper includes programs, concepts and details under continuing development by Cybersource. Any Cybersource features, functionality, implementation, branding, and schedules may be amended, updated or canceled at Cybersource's discretion. The timing of widespread availability of programs and functionality is also subject to a number of factors outside Cybersource's control, including but not limited to deployment of necessary infrastructure by issuers, acquirers, merchants and mobile device manufacturers. In addition, certain existing features are not available in all countries. Participation in programs and services are subject to Cybersource's terms and conditions in program participation agreements and associated documentation; acquirer participation, approval or sponsorship of merchant enrollment is required.

This whitepaper contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms "plan," "goal," "available," "may," "will" and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our roadmap, corporate strategy and product goals, plans and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including the following: the impact of legal and/or regulatory changes; disruptions to and/or problems with the development cycle; modifications to development priorities; and the other factors discussed under the heading "Risk Factors" in the Visa Inc., Cybersource's parent company, most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q. You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement, because of new information or future developments or otherwise.

Comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Cybersource does not make any warranty or representation as to the completeness or accuracy of the Information within this document, nor assume any liability or responsibility that may result from reliance on such Information. The Information contained herein is not intended as legal advice, and readers are encouraged to seek the advice of a competent legal professional where such advice is required.

All Revenue Capture initiatives* are implemented through Decision Manager, Cybersource's enterprise fraud management solution.

To learn more about Decision Manager and how your organization can implement Revenue Capture's industry-leading approach to optimizing authorization rates, contact Cybersource today at Cybersource.com.

*All initiatives are subject to change or cancellation at Cybersource's sole discretion.

cybersource
A Visa Solution