Cybersource Revenue Optimisation Solution for Crypto Exchanges

READ ON TO FIND OUT MORE →

cybersource
A Visa Solution

Contents

No reference to a business success is intended as an advertisement of advisory services. Each business experience is unique, so one business' success does not guarantee the same success for any future business. Past performance does not guarantee or indicate future results. Regions vary by market maturity, each region has its own unique fraud, payment landscape and use of Decision Manager.

Business challenge

Business challenge

Cryptocurrency exchanges are a prime target for fraud attacks, particularly when using fiat money to purchase cryptocurrency. The volatility and breadth of the marketplace coupled with rising consumer interest can create a growing market for fraud that exchanges must identify and help prevent.

The value and adoption of cryptocurrency has skyrocketed and will continue to grow as public awareness increases[1] due to things like television advertising, celebrity endorsements, and highly accessible mobile apps. This rapid growth creates a range of risks and has wide-reaching implications for payments, finance, and commerce.[2]

Cryptocurrencies' high value make them a desirable target for fraud attacks and generates scepticism from issuers and can result in lower authorisation acceptance rates.

Cryptocurrency exchanges can be the target of many attacks, leaving them to build out their underlying fraud infrastructure and authentication controls. Individual transactions such as purchases (conversion of fiat money to cryptocurrency) and the movement of funds between accounts place the exchange's revenue directly at risk—and can result from both stolen account information and friendly fraud.

Cybersource, a Visa solution, offers a solution that combats these challenges with an end-to-end suite of fraud and risk products and services that can mitigate fraud while maximising revenue. Cybersource Revenue Optimisation Solution can facilitate the movement of cryptocurrency without the associated customer experience challenges.

[1] Surging Interest Indicates Cryptocurrency is Becoming the Latest Wealth Accumulation Vehicle; https://www.prnewswire.com/news-releases/surging-interest-indicates-cryptocurrency-is-becoming-the-latest-wealth-accumulation-vehicle-301478751.html
[2] The Crypto Phenomenon: Customer Attitudes and Usage https://usa.visa.com/dam/VCOM/regional/na/us/Solutions/documents/the-crypto-phenomenon-technical-paper.pdf

Fraud trends

Fraud trends

The pandemic has been a universal disruptor, accelerating the need to adopt innovative payment solutions. Customers began to leverage new technologies and embrace DeFi, while businesses rushed to meet the needs of a remarkably different landscape, sometimes without the planning that normally comes with a dramatic strategy update. Fraudsters locked onto these changes and used their own innovations to execute attacks with a higher level of sophistication and determination than ever before. This came at a price, with 33% of the businesses surveyed by Cybersource in 2021 struggling to identify and respond to emerging fraud attacks and 28% lacking the data they need to manage fraud.[3]

Crypto exchanges, which offer the opportunity to exchange fiat currency for cryptocurrency and NFTs, are the most lucrative target for fraud in the cryptocurrency ecosystem with more than $26bn in disbursements in 2012.[4] Hot Cryptocurrency attracts a wide variety of fraud-related challenges from: stolen payment instruments and scams to "pump and dump" schemes designed to artificially inflate values to the friendly fraud of illegitimate "buyer's remorse."

Increased fraud costs have left many businesses prioritising fraud reduction over customer experience improvements without a corresponding increase in IT funding and efforts.[3] While manual review has historically been a common way to prevent fraud without IT changes, 60% of businesses surveyed want to reduce or eliminate their reliance on manual review for fraud prevention.[3] Accurate and automated fraud prevention that prioritises the customer experience is necessary to drive this change.

The more concerning issue is that issuers reject 18% of card-not-present (CNP) traffic, compared with 1% of card present (CP).[4] This affects crypto exchanges more acutely, in that businesses and exchanges experiencing high fraud volumes could have lower authorisation rates from issuers due to their perceived risk. Inconsistent issuer acceptance policies can lead to customer confusion, service issues, and even chargebacks. By reducing fraud with the Cybersource Revenue Optimisation Solution, businesses can positively influence issuer authorisation rates and improve customer experiences.

[3] 2022 Global Fraud and Payments Report; https://www.cybersource.com/en-ap/solutions/fraud-and-risk-management/fraud-report.html
[4] Cybersource Revenue Capture white paper; https://www.cybersource.com/content/dam/documents/en/cybersource-revenue-capture-whitepaper-2020.pdf

The strategy of revenue optimisation

A new way to look at maximising acceptance

Cybersource's strategy drives revenue optimisation by going beyond mitigating fraud risk and leading with acceptance—allowing you to recapture lost revenue by optimising authorisation conversions. As a pioneer in the payments industry, our optimisation solution helps increase revenue by leading with acceptance and minimising risk. Close partnership with a broad range of Visa teams and issuers enhances our fraud management tools, improves authorisation visibility, and reduces customer friction.

We're driven by five key initiatives

The Cybersource Revenue Optimisation Solution focuses on five key initiatives: preventing fraud, increasing visibility, pre-screening fraud, optimising tools, and enhancing the customer experience through automation.

- **Preventing fraud.** Fraud is costly to customers and businesses and carries reputational risk. Reducing chargebacks is a priority for eCommerce businesses, but it becomes more pressing in its impact on direct authorisation rates.[4] High chargeback rates can lead to penalties and reputational damage, but our Revenue Optimisation Solution can help lower chargeback rates to help boost issuer trust and strengthen authorisation acceptance rates.
- **Increasing authorisation rate visibility.** Although seamless authorisations are critical to the customer experience, only 30% of businesses are aware of their rates.[4] This makes it difficult to establish a baseline or identify opportunities for improvement. Our solution provides visibility through detailed authorisation rate reporting to enable proactive changes.
- **Pre-screening fraud.** Certain fraud attacks thrive on volume, throwing numerous attempted transactions at a business to see what succeeds. These high-volume attempts degrade authorisation rates. Our solution allows you to move fraud prevention upstream to pre-screen before authorisation, reducing the number of risky transactions sent to issuers, which in turn lowers decline rates.
- **Optimising tools.** Many fraud solutions rely on static models and manual processing. Cybersource recognises the dynamic nature of fraud and provides an ever-improving machine learning model that leverages Visa's entire network for insights. This includes 141 billion

transactions from VisaNet,[5] cross-merchant data, and data from other crypto exchanges. This allows the solution to determine the positive and negative qualities of events as they evolve with the fraud landscape. Our novel Replay feature lets you see the potential outcomes of planned strategy changes, which can help you reduce the pool of risky transactions that require further screening.

- **Enhancing customer experience through automation.** Today's customers expect an automated and seamless digital experience; and manual transaction review dramatically lowers conversion rates and causes customer escalations. Cybersource has fully integrated 3-D Secure capabilities into our Decision Manager tool with our Payer Authentication tool, enabling you to manage an end-to-end authorisation flow and transparent transaction reviews. You can filter out the majority of positive and negative transactions upfront, significantly reducing the number sent to manual review.

These principles are the backbone of the Cybersource Revenue Optimisation Solution. Together they provide the data and insight that gives businesses and issuers confidence in their decisions while also focusing on customer experience. How do we do it? Powered by industry-leading machine learning and artificial intelligence, and curated by insights from an experienced global team, Cybersource leads with automation and acceptance so that you can focus on growth.

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

Cybersource Revenue Optimisation Solution for cryptocurrency

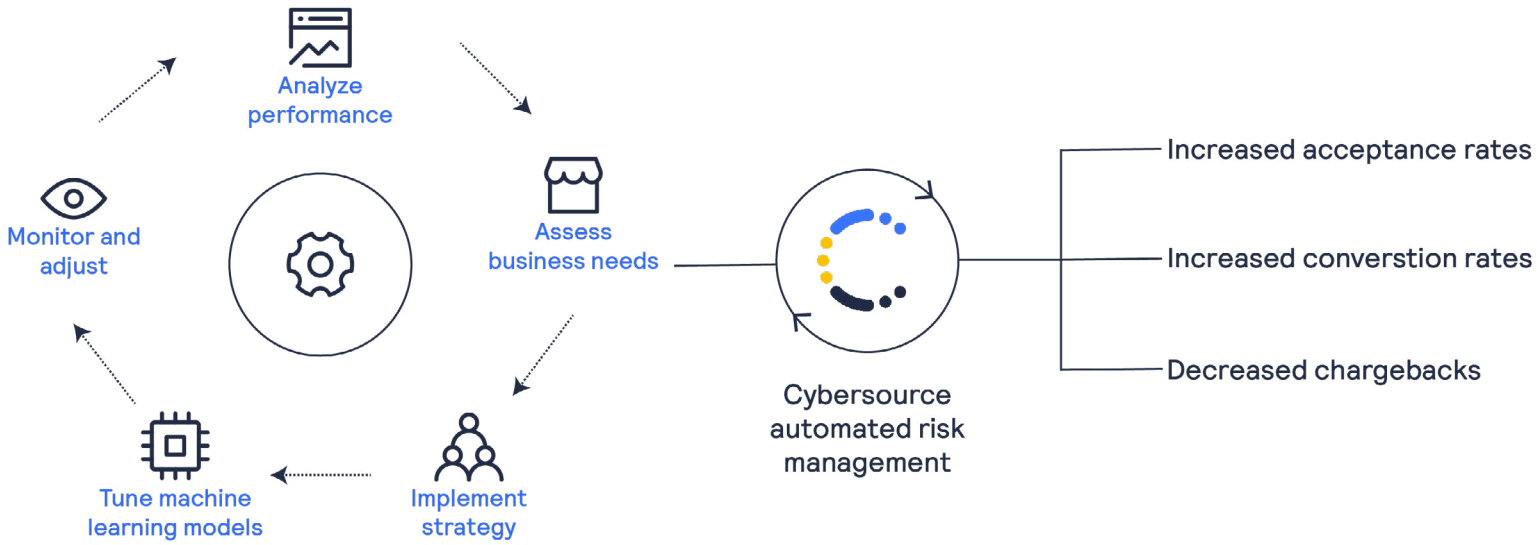
A new way to look at maximising acceptance

The Cybersource Revenue Optimisation Solution for cryptocurrency is all-inclusive and fully outsourced, optimising the flow of money of all forms in real time with advanced automation and one of the largest data networks. This combination of capabilities and unparallelled expertise allows businesses to innovate and drive new technologies without the overhead needed to maintain a of individual fraud solutions.

A layered approach

Fraud prevention is traditionally positioned as requiring a layered approach; businesses use at least four fraud products on average.[3] Implementing this kind of layering can be costly and time-consuming and uses up valuable IT capacity. As an alternative, to avoid managing multiple providers and platforms, Cybersource offers the simplicity of a single, end-to-end platform that leverages machine learning and AI to automate risk management. It is easy to implement and fully integrated, with device profiling, 3DS authentication capabilities, and third-party data services. Our solution is flexible, scalable, automated, and comes through a single connection and a single provider with the ability to share learnings across tools.

Fraud attacks are constantly changing and introducing new variables, so analysing performance is an ongoing process. Our solution is focused on increasing acceptance rates and reducing fraud by understanding your unique use cases, implementing a strategy to maximise revenue, fine-tuning with industry-leading machine learning risk models, and adjusting as needed to reach optimisation.

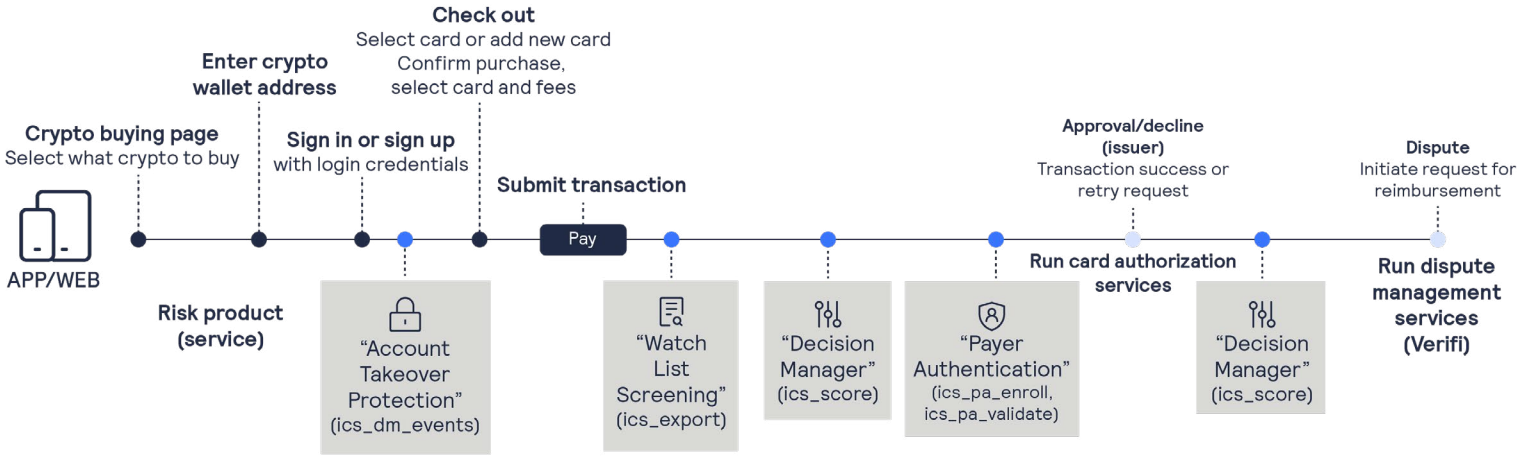


Cybersource Revenue Optimisation Solution for cryptocurrency

A new way to look at maximising acceptance

An end-to-end solution

Your business is unique, which means your fraud risks and attacks are unique too. Each layer in our solution can be customised to your needs, creating a fully customised and dynamic fraud prevention strategy that closely monitors performance. The solution provides reporting and analytics that reflect your goals to enable full ongoing visibility.



You can also leverage the expertise of our specialised risk consultants, who ensure careful end-to-end planning based on the broad knowledge they have developed from working with a diverse client base. All these components link together to create a preventative framework that matches your specialised risks and that can adapt even quicker than some fraud attacks.

Revenue Optimisation Solution tools

Account Takeover Protection

Account Takeover Protection

Fraud attacks are more sophisticated than ever, and fraudsters have moved higher upstream.
Rather than reacting to past attacks, our Account Takeover Protection solution can detect fraud early and at the account level. In combination with our revenue optimisation solution, complementing your strategy to provide protection from account setup through checkout.

Account Takeover Protection provides a flexible rules engine that identifies indicators of suspicious activity based on behaviour, email, device, communications, and other predictive attributes. With these behavioural indicators, you can identify and block not only traditional account takeover fraud but also fake account creation, loyalty fraud, and other pre-transaction attacks. For example, comparing the device details used at account creation with those used in a chargeback could allow exchanges to successfully dispute friendly fraud fiat chargebacks from established customers.

Key benefits

Preserve customer trust and brand loyalty

Your brand reputation pays the price for stolen customer credentials, even if the breach happened elsewhere. By preventing these attacks, Account Takeover Protection keeps your customers and reputation safe.

Prevent bad transactions before they take place

The fraudulent transactions that result from account takeover come with chargebacks, loss of inventory, and dispute resolution costs. Identifying account fraud reduces related costs downstream.

Avoid customer attrition

Just one account-related fraud event can erode customer trust and cause costly attrition.

Revenue Optimisation Solution tools

Watch List Screening and Chargeback management

Watch List Screening

Cybersource's Watch List Screening enables businesses to incorporate economic sanctions, counterterrorism, money laundering, and denied parties lists in real time through the Watch List Screening verification service. You can easily compare purchaser information with regulatory lists to ensure you are making compliant decisions and preventing exchanges' use in money laundering.

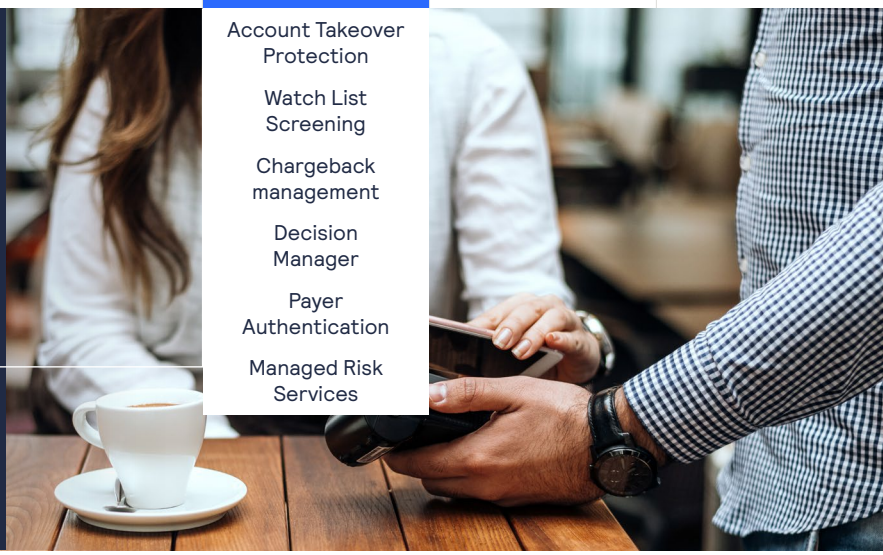
The Watch List Screening tool includes 23 regularly updated sanction lists that allow you to screen across multiple regulatory organisations and connect matches in a single step. Its matching algorithm compares business information with the lists but also includes configurable logic to refine the review, minimising errors and false positives.

Chargeback management

Chargeback management, provided by Verifi, a Visa Solution, is an important step in the cycle of preventing fraud and perfecting controls. Knowing which chargebacks to dispute as well as how to dispute them requires specialised knowledge and skills. In conjunction with the other tools, Verifi's chargeback management increases the chances of winning costly chargeback disputes.

Revenue Optimisation Solution tools

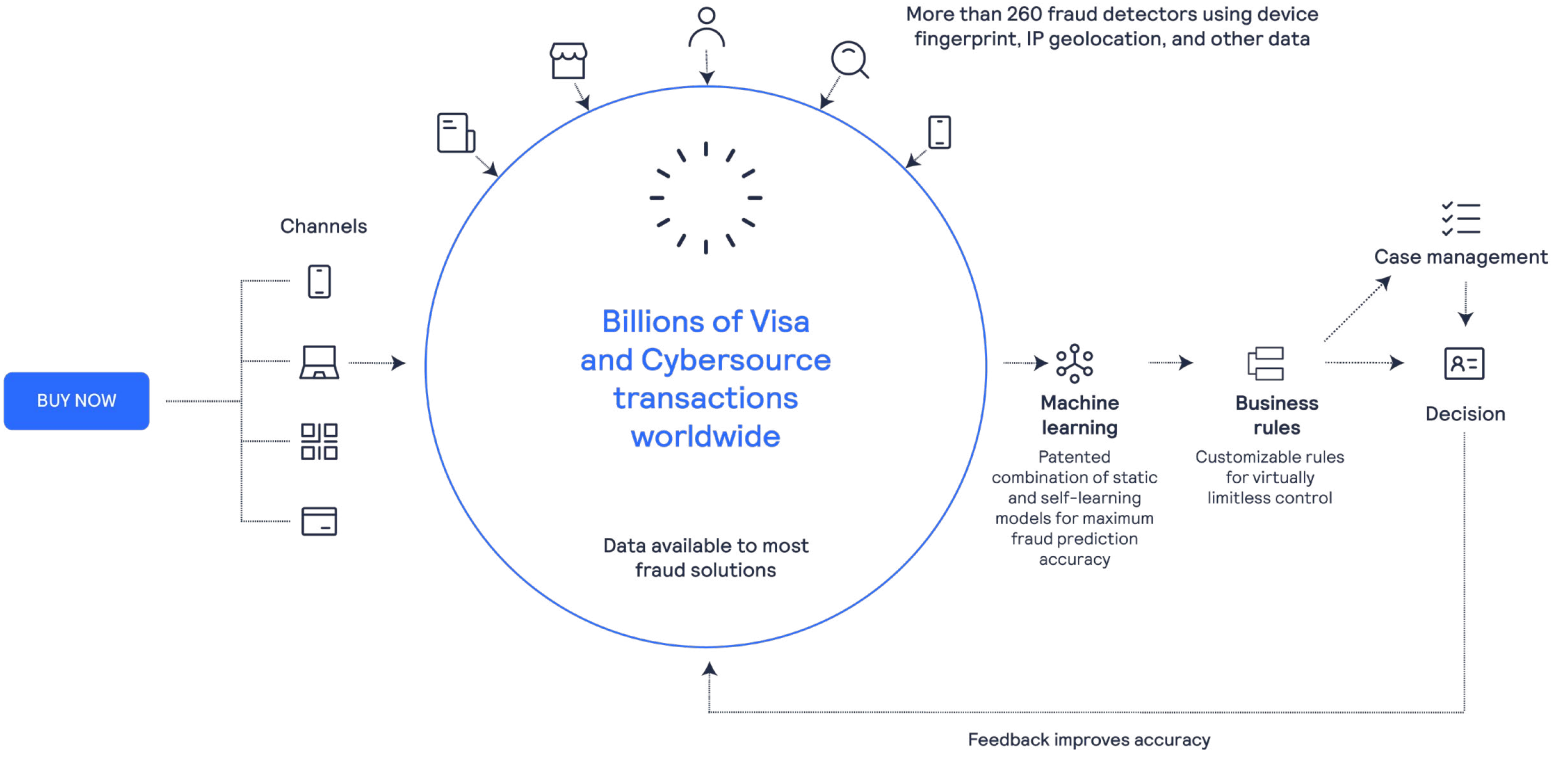
Decision Manager



Decision Manager is Cybersource's flagship fraud and risk management solution, combines global fraud behavioural modelling, decades of payment and risk knowledge, and the integrity of Visa's network. Its robust capabilities allow businesses to make transaction decisions using a range of sophisticated machine learning models. **In addition to AI-powered fraud prevention, Decision Manager houses a fully customisable rules engine, a case management system, analysis tools, and a real-time reporting portal. It's available as a standalone service or fully integrated with the Cybersource payment management platform to deliver even stronger results.**

Decision Manager uses multiple machine learning models in conjunction with customised fraud rules leading to greater flexibility and accuracy. Its ability to ingest a broad range of data and convert it into understandable human behaviour insights allows for careful filtering of high-risk transactions prior to issuer submission. Cryptocurrency is a prime target for fraud, and many traditional solutions aren't equipped to combat these unique cryptocurrency attacks.

Increased conversion rates following the implementation of Decision Manager both pre- and post-authorisation can also result in an increase in authorisation rates from issuers. By decoupling the fraud check from the authorisation call, exchanges are given the flexibility to mindfully allow the most profitable transactions at the right time. These positive outcomes across all transaction types drive top-line growth and improved customer experience.



Decision Manager's multiple models also pinpoint positive behaviours, and its advanced machine learning models analyse historical transaction data to parse fraudulent and valid transactions. While a customer might be new to the cryptocurrency market, it's highly likely that their digital identity has already been seen on Visa's far-reaching network. Decision Manager gives you the control to balance accurate automation with precision custom rule sets. By acting as the focal point for a full suite of fraud prevention layers, Decision Manager helps reduce fraud rates, encourage liquidity, and drive sales innovation and growth through a single integration.

Key features

Identity Behaviour Analysis

Insights from the broader global business consortium allow businesses to quickly segment risk from good business, accelerating prevention and promoting confidence around the acceptance of genuine and recurring transactions.

Rules Suggestion Engine

Turn the power of machine learning into fraud analysis based on your unique transaction history to recommend rules that augment and improve your existing strategies. Each suggestion is accompanied by detailed metrics that enable you to estimate performance.

DM Replay

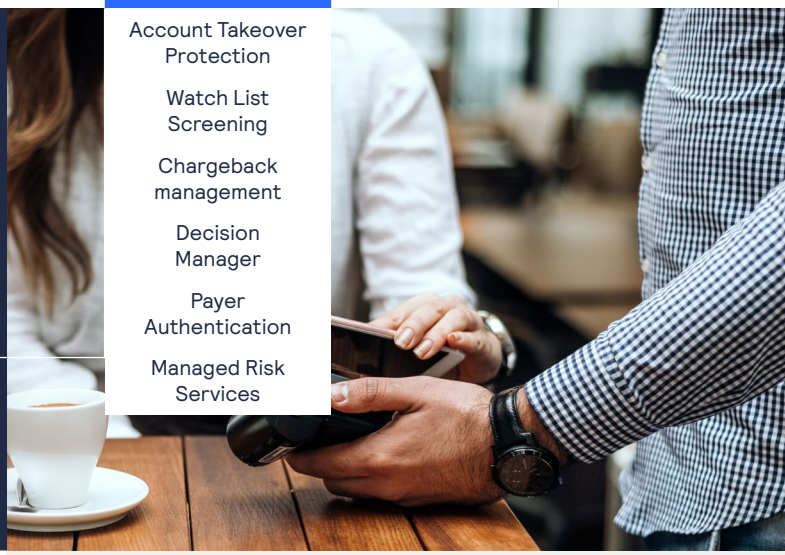
The impact of potential changes can be assessed in real time prior to going live using Replay. Its innovative technology enables rapid changes and provides the confidence needed to implement new strategies.

Third-party integrations

Built-in partnerships give you the ability to instantly integrate with additional global fraud services without the associated IT development costs. Potential partners include digital identity, behavioural biometric, and email and identity verification data resources.

Revenue Optimisation Solution tools

Payer Authentication



Payer Authentication deters unauthorised payment card use and protects against fraudulent chargebacks. This integrated service uses the EMV® 3-D Secure (3DS) protocol for authentication and leverages the 3DS server to provide multi-step authentication that turns away the riskiest attempts to buy cryptocurrencies before issuers even see the transaction.

Using Payer Authentication with Decision Manager allows a more streamlined approach to 3DS authentication. Decision Manager can automatically route transactions to authentication, with the ability to pause those that are high-risk transactions and require a step-up challenge from the issuer. After the step-up challenge is successfully completed, without requiring another call, it captures the authentication results and resumes the transaction by proceeding to authorisation.

Using Decision Manager plus Payer Authentication provides an additional layer of protection, enhances decision-making with authentication insights, and gives you a more streamlined approach to supporting 3DS.

Key benefits

Add a layer of risk protection by leveraging 3DS

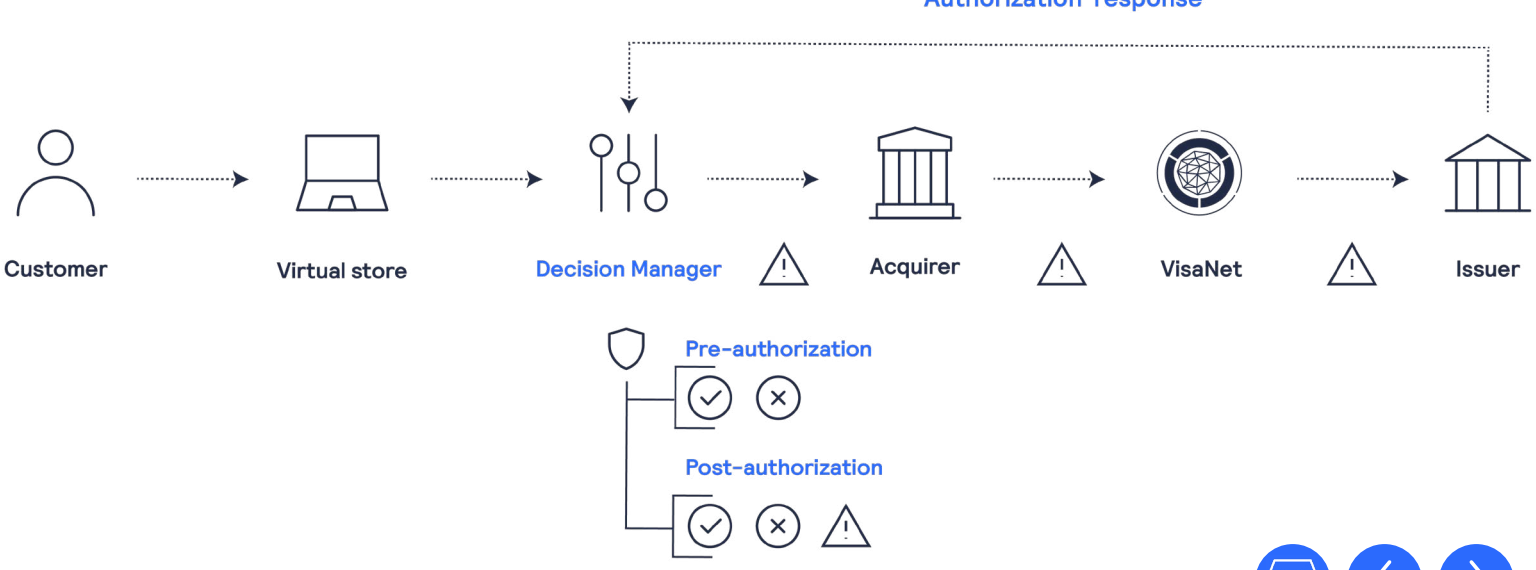
- Automatically route transactions through for authentication
- High-risk transactions may receive an additional challenge from issuers

Shift liability

Issuing banks become liable for fraud chargebacks verified with Payer Authentication

Raise authorisation rates

Sending authenticated transactions to authorisation gives issuers greater confidence for approval



Revenue Optimisation Solution tools

Managed Risk Services

Cybersource's Managed Risk Services bring together all the components of our Revenue Optimisation Solution under a dedicated fraud expert

Our Managed Risk Analysts work to quickly understand your unique needs while staying on the leading edge of cryptocurrency risks and study the business models of a range of exchanges.

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. This has left many businesses feeling that they cannot keep up with emerging fraud trends and support the day-to-day; let a Cybersource Managed Risk Analyst focus on fraud while you focus on business needs.

Key benefits

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

Proven results with a trusted partner

As trailblazers in fraud prevention, Cybersource and Visa are experienced partners that enable businesses to innovate while meeting their unique fraud prevention needs. The strength of Visa's infrastructure and extensive data consortium brings a stable and widely knowledgeable backbone to this flexible and powerful solution. The Cybersource Revenue Optimisation Solution for cryptocurrency enables a partnership that will improve your fraud prevention performance and allow you to safely boost DeFi adoption.

The Cybersource Revenue Optimisation Solution for cryptocurrency produces exceptional results. Businesses that optimised their acceptance strategies with Cybersource [6]:

- Saved $4m in manual review costs
- Increased acceptance by $36.8M
- Maintained stable performance during market volatility
- Experienced exceptional 99.997% uptime
- Increased authorisation rates by 1%
- Increased acceptance rates by 8%

cybersource
A Visa Solution

[6] Disclosures: Results calculated using internal data based on Decision Manager clients in North America during the January 2020 to November 2021. Results will vary based on factors including if client works with Cybersource Managed Risk Services and how client uses Decision Manager. Average cost to review a transaction for is US $3.

Definitions

Cryptocurrency
A digital asset that can be used as a store of value or a medium of exchange for goods and services. Transactions are verified and recorded using cryptography by a distributed network of participants, rather than a centralised authority such as a bank or government agency.

DeFi
Short for decentralised finance. Finance is traditionally centralised because it relies on trusted intermediaries. For example, if you want to send money to a friend or relative, you rely on your bank to send it to the recipient's bank. DeFi, on the other hand, requires no intermediaries. Participants can send and receive assets directly. In theory, this makes transactions faster and cheaper.

Exchange
A website or app that allows users to buy and sell crypto assets.

Fiat currency
Traditional currencies are backed by the full faith and credit of a nation state. The U.S. dollar, the euro or the British pound are fiat currencies.

NFT
An acronym that stands for a non-fungible token, a digital collectible that uses the same underlying technology as cryptocurrencies.

Get in touch with us to find out how.

› Contact us

cybersource
A Visa Solution