Cybersource 加密货币交易平台营收优化解决方案

业务挑战 →

营收优化策略 →

加密货币解决方案 →

工具 →

来自值得信赖的合作伙伴的可靠结果 →

请点击此处了解详情 →

cybersource
A Visa Solution

目录

业务挑战

业务挑战

加密货币交易平台是欺诈攻击的主要目标，特别是在使用法定货币购买加密货币时。市场的波动性和广度，加上消费者兴趣上升，可能会导致欺诈市场的增长，交易平台必须识别并帮助防范欺诈。

受电视广告、名人代言以及快速、便捷的移动应用程序等因素的影响，加密货币的价值和采用率急剧上升[1]，并将继续增长。这种快速增长产生了一系列风险，并对支付、金融和商业产生了广泛影响。[2]

加密货币的高价值使其成为欺诈攻击的理想目标，引起发卡行的怀疑，并可能导致授权成功率降低。

加密货币交易平台可能成为许多攻击的目标，迫使其建立自己的基础反欺诈基础架构和验证控制措施。个人交易，如购买（法定货币转换为加密货币）和账户之间的资金流动，将交易平台的营收直接置于风险之中——原因可能是账户信息被盗和伪善欺诈。

Cybersource，Visa 旗下的平台，通过一套端到端反欺诈和风险产品和服务，提供了一种应对这些挑战的解决方案，可以在减少欺诈的同时最大限度增加营收。Cybersource 营收优化解决方案可以促进加密货币的流动，而不会给客户体验带来挑战。

[1] 人们对加密货币的兴趣飙升，表明加密货币正成为最新的财富积累工具
[2] 加密货币现象：客户态度和使用情况

欺诈趋势

欺诈趋势

疫情是一个普遍性的干扰因素，正在加快对采用创新支付解决方案的需求。客户开始利用新技术并接受 DeFi，而企业则急于满足一个截然不同的环境需求，有时甚至没有进行通常伴随着重大策略更新的规划。欺诈者锁定了这些变化，并使用他们自己的创新以前所未有的复杂程度和决心发起攻击。这是有代价的，在 2021 年接受 Cybersource 调查的企业中，有 33%的企业难以识别和应对新出现的欺诈攻击，28% 的企业缺乏管理欺诈所需的数据。[3]

加密货币交易平台提供了将法定货币兑换为加密货币和 NFT（非同质化代币）的机会，是加密货币生态系统中最有利可图的欺诈目标，2012 年支付的金额超过 260 亿美元。[4]热门的加密货币招致各种各样的欺诈相关挑战：从盗用支付工具和诈骗到旨在人为抬高价值的“哄抬股价”计划，到非法“买家懊悔”伪善欺诈。

欺诈成本增加使许多企业将减少欺诈置于改善客户体验之上，而没有相应增加 IT 方面的资金投入和措施。[3]虽然过去人工审核一直是在不进行 IT 变更的情况下防范欺诈的常见方法，但 60% 的受访企业希望减少或消除对用于防范欺诈的人工审核的依赖。[3]将客户体验放在首位的准确的自动化欺诈防范，对于推动这一变更必不可少。

更令人担忧的问题是，发卡行拒绝 18% 的无卡交易 (CNP)，相对而言只拒绝 1% 的有卡交易 (CP)。[4] 这对加密货币交易平台的影响更为严重，因为经历大量欺诈的企业和交易平台可能因为其可感知的风险而获得更低的发卡行授权率。不一致的发卡行接受政策可能导致客户混淆、服务问题甚至拒付。企业通过使用 Cybersource 营收优化解决方案减少欺诈，可以积极影响发卡行授权率并改善客户体验。

[3] 2022 年全球反欺诈和支付报告
[4] Cybersource 营收获取白皮书

营收优化策略

最大限度提高接受率的新方式

Cybersource 的策略是通过降低欺诈风险以及实现领先的接受率来推动营收优化，从而允许您通过优化授权转换来收复营收失地。作为支付行业先锋，我们的优化解决方案通过实现领先的接受率以及风险最小化来帮助增加营收。通过与众多 Visa 团队和发卡行建立密切合作，可增强我们的反欺诈管理工具，提高授权率可见性并减少客户打扰。

我们通过五项关键计划推动这一解决方案的实施

Cybersource 营收优化解决方案重点关注五项关键计划：防范欺诈、提高可见性、预筛查欺诈、优化工具，以及通过自动化增强客户体验。

- 防范欺诈。欺诈会让客户和企业付出高昂代价，并会带来声誉风险。减少拒付是电子商务企业的首要任务，但由于它对直接授权率的影响而变得更为紧迫。[4] 高拒付率可能导致罚款和声誉受损，但我们的营收优化解决方案可以帮助降低拒付率，以帮助提高发卡行的信任以及授权接受率。
- 提高授权率可见性。尽管无缝授权对客户体验至关重要，但只有 30% 的企业知道这类授权的授权率。[4] 因此很难建立一个基线或确定改进的机会。我们的解决方案通过详细的授权率报告提供可见性，以支持主动变更。
- 预筛查欺诈。某些欺诈攻击以量取胜，向企业抛出大量尝试进行的交易，看看哪些交易能成功。这些大量尝试会降低授权率。我们的解决方案允许您将反欺诈上游移动到授权前的预筛查，减少发送给发卡行的风险交易数量，从而降低拒绝率。
- 优化工具。许多反欺诈解决方案依赖于静态模型和人工处理。Cybersource 认识到欺诈的动态性质，提供一种不断改进的机器学习模型，利用整个网络获取相关见解，包括来自 VisaNet 的 1410 亿笔交易[5]、跨商户数据和来自其他加密货币交易平台的数据，允许解决方案确定事件为积极性质还是消极性质，因为它们会随着欺诈环境的发展而变化。我们全新的 Replay 功能可以让您看到计划中的策略变更的潜在结果，帮助您缩小需要进一步筛查的风险交易池。

[4] Cybersource 营收获取白皮书
[5] VisaNet 2020 财政年度交易量。交易量可能不包括国内交易。

- 通过自动化增强客户体验。T如今的客户期待的是顺畅无碍的自动化、数字化体验；人工交易审核极大地降低了转化率，并导致客户问题升级。[5] Cybersource 将 3-D Secure 功能完全集成到 Decision Manager 工具以及付款人身份验证中，使您能够管理端到端流程和透明化交易审核，并可以预先过滤掉大部分良好交易和不良交易，显著减少发送进行人工审核的交易数量。

这些原则是 Cybersource 营收优化解决方案的基础。它们共同提供数据和见解，让企业和发卡行对自己的决策有信心，同时也关注客户体验。我们是如何做到的呢?Cybersource 以业界领先的机器学习和人工智能为基础，并采用经验丰富的全球团队的见解进行组织策划，提供领先的自动化和接受率，使您可以专注实现增长。

Cybersource 加密货币营收优化解决方案

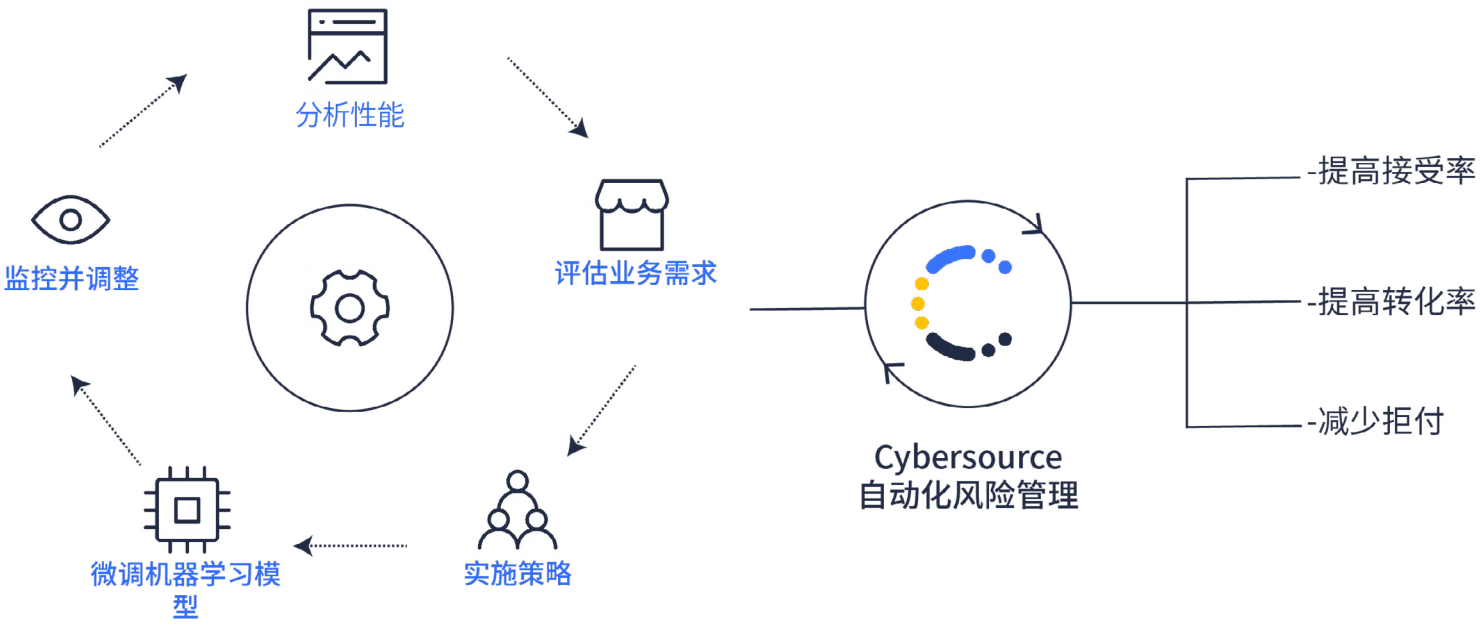
最大限度提高接受率的新方式

Cybersource 加密货币营收优化解决方案一价全包且完全外包，通过先进的自动化和最大的数据网络之一实时优化所有形式的资金流。这种功能和无与伦比的专业知识相结合，使企业可以在无需维护单个反欺诈解决方案的情况下实现新技术的创新和发展。

分层方法

F防范欺诈在传统意义上定位为需要采用分层方法；企业平均使用至少四种反欺诈产品。[3] 实施这种分层可能价格昂贵且耗时，并且会耗尽宝贵的 IT容量。作为一种备选方案，为了避免管理多个供应商和平，Cybersource 提供一款简单的端到端平台，利用机器学习和 AI 实现风险管理的自动化。该平台易于实施且完全集成，提供设备分析、付款人身份验证功能以及第三方数据服务。我们的解决方案具有灵活、可扩展和自动化的特点，通过单一连接和提供商来实现跨工具共享学习成果的能力。

欺诈攻击在不断变化并引入新的变量，因此对性能的分析是一个持续的过程。我们的解决方案专注于了解您的独特用例、实施营收最大化策略、使用业界领先的机器学习风险模型进行微调，并根据需要进行调整以达到优化，从而提高接受率并减少欺诈。

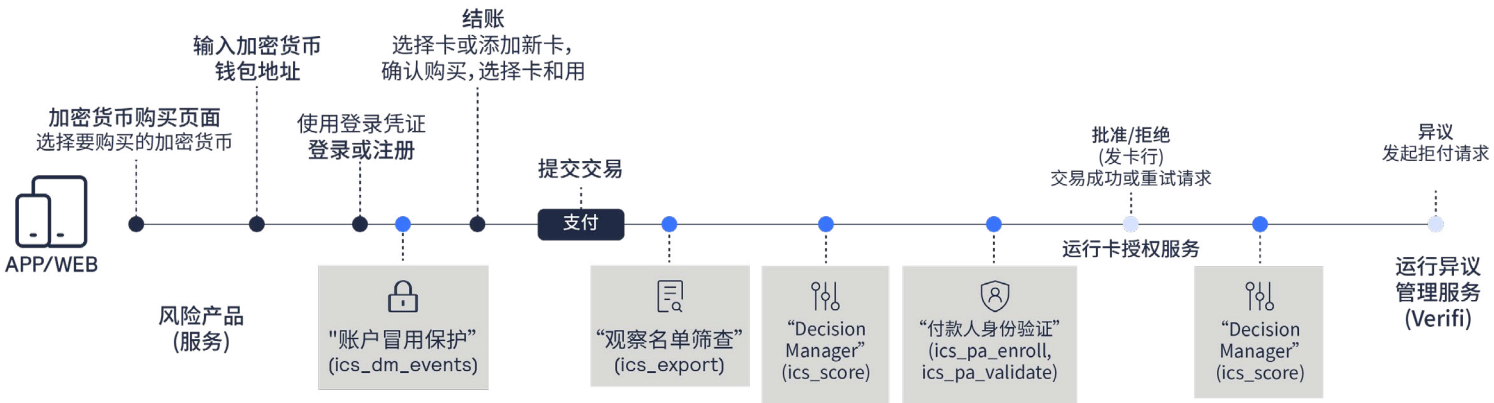


Cybersource 加密货币营收优化解决方案

最大限度提高接受率的新方式

端到端解决方案

您的业务独一无二，这意味着您遇到的欺诈风险和攻击也独一无二。我们的解决方案中的每一层都可以根据您的需求进行定制，创建一个完全定制的动态反欺诈策略，密切监控性能。该解决方案提供反映您目标的报告和分析，以全面实现持续的可见性。



您还可以利用我们的专业风险顾问所具备的专业知识，他们根据与不同客户群合作积累的广泛知识，确保提供谨慎的端到端规划。所有这些部分连接在一起，创造出一个与您的专业风险相匹配的防范框架，适应速度甚至比一些欺诈攻击更快。

营收优化解决方案工具

账户冒用保护

账户冒用保护

欺诈攻击的复杂程度前所未有，并且欺诈者已移至上游端。

我们的账户冒用防范解决方案可以在早期和账户层面检测欺诈，而不是对过去的攻击作出反应。结合我们的营收优化解决方案，补充您的策略，以提供从账户设置到结账的全程保护。账户冒用保护提供一个灵活的规则引擎，可根据行为、电子邮件、设备、通信和其他预测属性识别可疑活动指标。有了这些行为指标，您可以识别和阻止的不仅包括传统的账户冒用欺诈，还包括虚假账户创建、忠诚度欺诈和其他交易前攻击。例如，将账户创建时使用的设备详细信息与拒付时使用的设备详细信息进行比较，可以使交易平台成功对来自现有客户的伪善欺诈法定货币拒付提出异议。

主要优势

维护客户的信任度和品牌忠诚度。

您的品牌声誉会因客户凭证遭窃而受损，即使窃取发生在其他地方。账户冒用保护通过防止这些攻击，保护您的客户和声誉的安全。

阻止不良交易的发生。

账户冒用导致的欺诈性交易伴随着拒付、库存损失以及解决异议的成本。识别账户欺诈可降低下游的相关成本。

避免客户流失。

只要发生一起与账户相关的欺诈事件，就会降低客户的信任，造成代价高昂的客户流失。

营收优化解决方案工具

观察名单筛查与拒付管理

观察名单筛查

Cybersource 的观察名单筛查使企业能够通过观察名单筛查验证服务，将经济制裁、反恐怖主义、洗钱和贸易管制名单实时纳入其中。您可以轻松地将买方信息与监管名单进行比较，以确保您做出符合规定的决策，并防止交易平台用于洗钱。

观察名单筛查工具包括 23 个定期更新的制裁名单，允许您跨多个监管组织进行筛查，并且一步关联匹配。所采用的匹配算法将企业信息与名单进行比较，但还包括可配置逻辑，以优化审核，最大程度减少错误和误报。

拒付管理

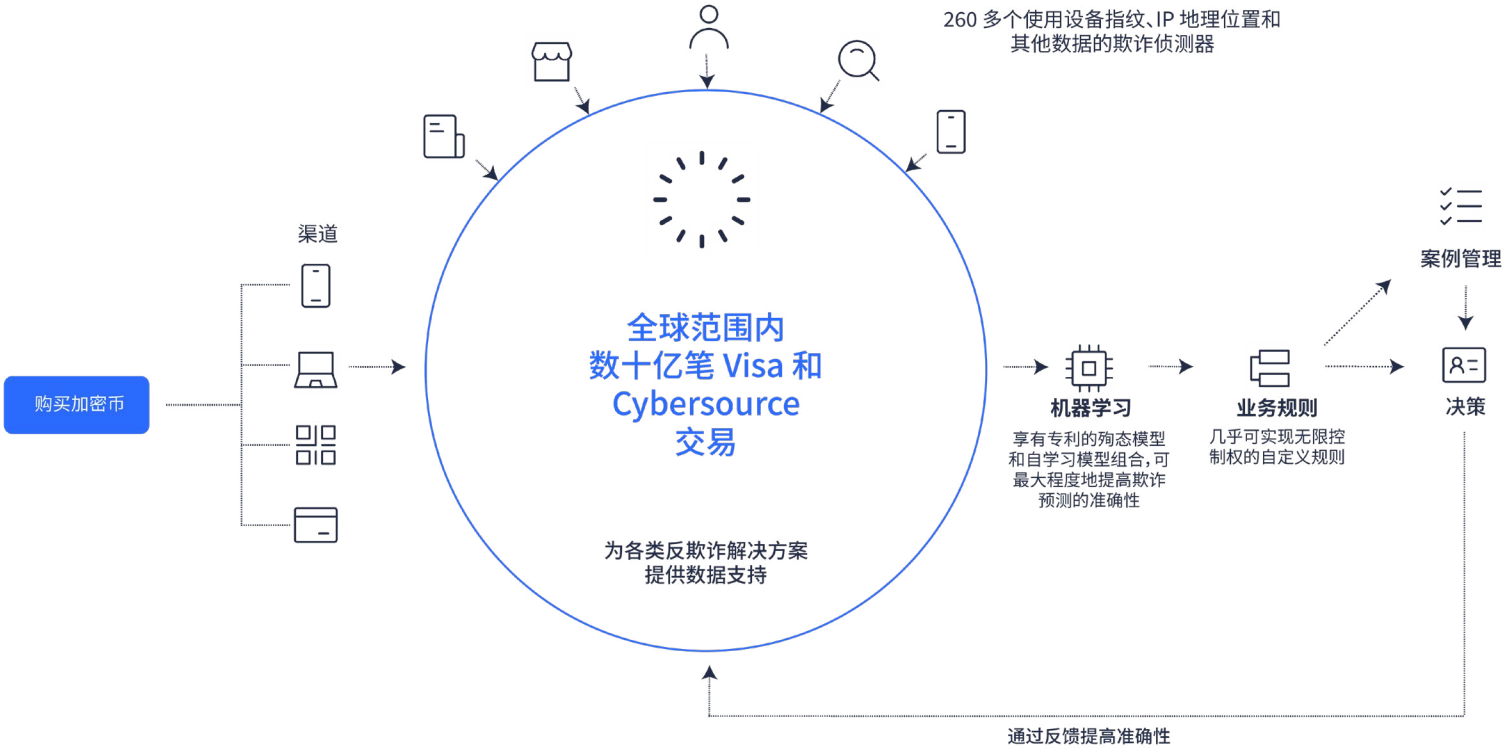
由 Visa 解决方案 Verifi 提供的拒付管理是防范欺诈和完善控制循环中的重要一步。要识别对哪些拒付提出异议以及如何提出异议，需要具备专业知识和技能。Verifi 的拒付管理搭配使用其他工具，增加了赢得代价高昂的拒付异议的几率。

营收优化解决方案工具

Decision Manager

Decision Manager 是 Cybersource 的旗舰级反欺诈及风险管理解决方案，综合运用了全球欺诈行为模型、数十年的支付和风险知识以及完整的 Visa 网络。该产品提供多种强大的功能，允许企业使用一系列复杂的机器学习模型来做出交易决策。**除基于人工智能的欺诈防范外，Decision Manager 还包含一个可完全定制的规则引擎、一个案例管理系统、分析工具和一个实时报告门户网站。它可以作为一项独立的服务，也可以与 Cybersource 支付管理平台充分集成，以提供更强大的结果。**

Decision Manager 使用多种机器学习模型，结合定制的反欺诈规则，可带来更大的灵活性和准确性。它能够摄取广泛的数据，并将其转换为可理解的人类行为见解，从而实现在发卡行提交之前仔细过滤高风险交易。加密货币是欺诈的主要目标，许多传统解决方案无法应对这些独特的加密货币攻击。



在预授权和后授权实施 Decision Manager 后，转化率将会提高，这也会使发卡行授权率增加。通过将欺诈检查与授权通话分离，交易平台可以在正确的时间灵活、谨慎地准许最有利可图的交易。所有交易类型的这些积极成果推动了营业额增长并改善了客户体验。

主要特色

Identity Behavior Analysis

通过从更广泛的全球企业联合体获得的见解，企业能够迅速从良好业务中分离风险，加速防范，并提升对接受真实交易和重复性交易的信心。

Rules Suggestion Engine

根据您独特的交易历史，将机器学习的力量转化为欺诈分析，以推荐增强并改进您现有策略的规则。每个建议都附带详细的指标，让您能够评估绩效。

DM Replay

通过 Replay 上线之前，可以实时评估潜在变更的影响。它的创新技术使快速变更成为可能，并提供实施新策略所需的信心。

第三方集成

凭借内置合作伙伴关系，您能够立即与其他全球反欺诈服务集成，而无需付出相关的 IT 开发成本。潜在的合作伙伴包括数字身份、行为生物识别以及电子邮件和身份验证数据资源。

营收优化解决方案工具

付款人身份验证

付款人身份验证可防止未经授权使用支付卡并防范欺诈性拒付。这一集成式服务采用 EMV® 3-D Secure (3DS)协议进行认证，并利用 3DS 服务器提供多步骤认证，在发卡行看到交易之前，将购买加密货币的风险企图拒之门外。通过将付款人身份验证与 Decision Manager 结合使用，可使付款人身份验证方法更加精简。Decision Manager 可以自动路由交易以进行验证，并能够暂停高风险交易以及需要发卡行升级质询的交易。在无需另一个通话的情况下成功完成升级质询之后，它将捕获验证结果，并通过继续进行授权来恢复交易。使用 Decision Manager 和付款人身份验证可提供额外的保护层，通过验证见解增强决策，并为支持 3DS 提供更精简的方法。

主要优势

利用 3DS 增加一层风险保护

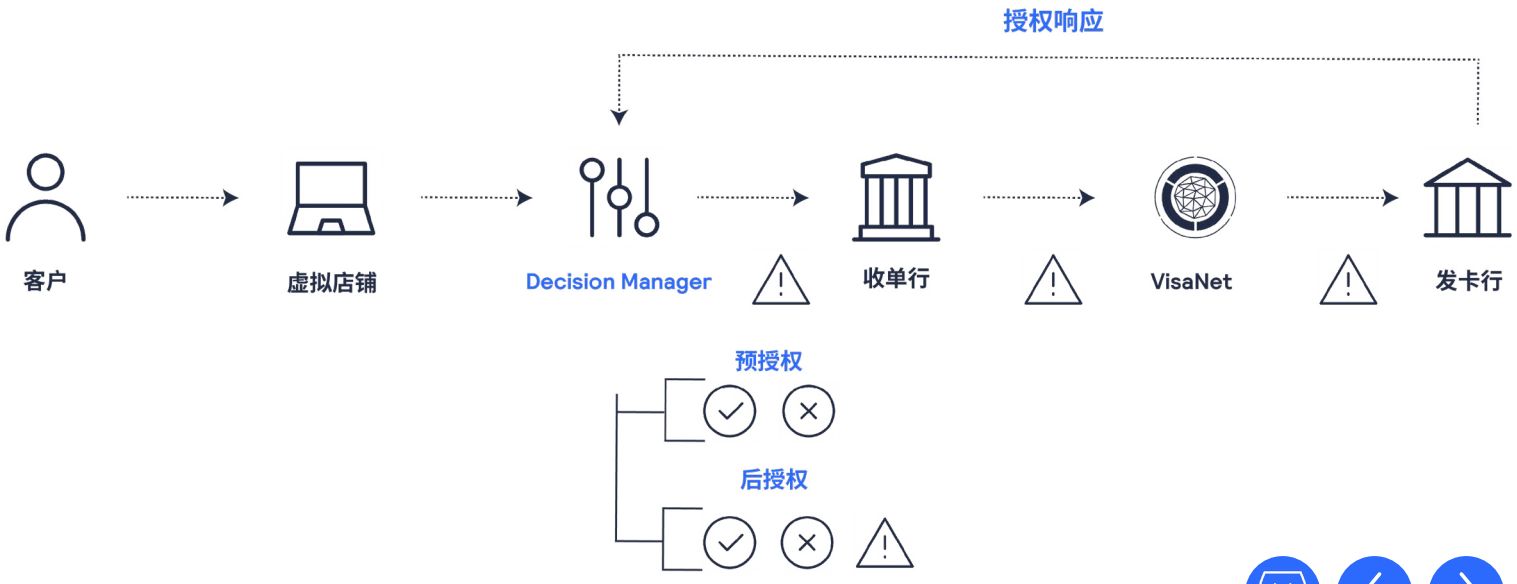
- 自动路由交易以进行验证。
- 高风险交易可能会受到来自发卡行的额外质询 。

转移责任

发卡行对经付款人身份验证检验的欺诈拒付承担责任。

提高授权率

将经过验证的交易发送给授权机构，使发卡行更有信心进行批准。



营收优化解决方案工具

托管式风险服务

在专业的反欺诈专家的带领下，Cybersource的托管式风险服务将我们的营收优化解决方案的所有部分融为一体。

我们的托管式风险分析师致力于快速了解您的独特需求，同时在管理加密货币风险方面保持领先，并研究一系列交易平台的业务模式。如今，反欺诈管理者有望身兼多职，包括运营、营销、物流、支付、异议和客户服务，并且通常被视为未来业务增长的“守护者”。这让许多企业感到无法跟上新出现的欺诈趋势，且无法维持日常运作；让 Cybersource 托管式风险分析师专注于防范欺诈，而您专注于满足业务需求。

主要优势

- 提供性能监控
- 执行分析，获得见解
- 调整反欺诈策略
- 利用专业的反欺诈产品
- 应用身份和电子邮件见解
- 了解不断变化的欺诈环境
- 充当值得信赖的反欺诈资源

与值得信赖的合作伙伴一起取得可靠的结果

作为欺诈防范领域的先驱，Cybersource和Visa 是经验丰富的合作伙伴，能够在满足企业独特的欺诈防范需求的同时，帮助企业进行创新。Visa 强大的基础设施和广泛的数据联合体为这个灵活而强大的解决方案带来了稳定和广泛的知识基础。Cybersource 加密货币营收优化解决方案支持通过合作提高您的反欺诈效果，并允许您安全地提高 DeFi 的采用。

Cybersource 加密货币营收优化解决方案成果卓越。通过 Cybersource 优化接受策略的企业[6]：

- 节省了 400 万美元人工审核成本
- 接受的金额提高了 3680 万美元
- 市场波动期间保持稳定绩效
- 正常运行时间高达 99.997%
- 授权率提高 1%
- 接受率提高 8%

cybersource
A Visa Solution

[6] 资料来源：使用基于 2020 年 1 月至 2021 年 11 月期间北美 Decision Manager 客户的内部数据计算所得结果。结果将根据客户是否使用 Cybersource 托管式风险服务以及客户使用 Decision Manager 的方式等因素而有所不同。审核一笔交易的平均成本是 3 美元。

定义

加密货币
一种可以用作保值以及产品和服务交换媒介的数字资产。交易由分布式参与者网络通过加密技术进行验证和记录，而非由银行或政府机构等集权机构进行验证和记录。

DeFi
分散式金融的简称。传统意义上的金融是集中的，因为它依赖于可靠的中间商。例如，如果您想给一个朋友或亲戚汇款，您会依靠您的银行将钱汇到收款人的银行。另一方面，DeFi 无需中间商。参与者可以直接发送和接收资产。理论上，这可以加快交易速度并降低成本。

交易平台
允许用户买卖加密货币资产的网站或 App。

法定货币
由国家的充分信任和信用提供支持的传统货币。美元、欧元或英镑都属于法定货币。

NFT
这是一个首字母缩略词，代表不可替代代币，这是一种使用与加密货币相同的底层技术的数字收藏品。

请联系我们了解详情。

› Cybersource.com

cybersource
A Visa Solution

