营收捕手

新一代电子商务支付和反欺诈管理

cybersource
A Visa Solution

目录

Cybersource 成立于 1994 年，是全球首批电子商务支付管理公司之一。作为线上支付处理和反欺诈管理领域的先行者，Cybersource 服务于大中型企业二十余年，提供完备的电子商务支付解决方案组合。2010 年，Cybersource 成为 Visa, Inc. 的全资控股子公司。如今，全球有超过 450,000 家企业依托 Cybersource 简化其线上支付解决方案。[1]

1. 截至 2020 年 6 月 2 日。包括 Authorize.Net 业务。

反欺诈的新前线：与发卡行合作提高授权率

电子商务营收目前大约每 4.5 年翻一番，[2] 但若要利用这种增长，则需采取细致入微的方法管理电子商务交易，以帮助发卡行更放心地接受更多授权请求。

2. 假设继续保持 15% 的电子商务平均增长率；利用通过 Digital Commerce 360 “2019 年美国电子商务销售额增长 14.9%” 得出的 2010-2019 年同比增长率计算。请参阅：https://www.digitalcommerce360.com/article/us-ecommerce-sales/。估算未考虑新冠疫情对电子商务的影响。

反欺诈管理：
历史回顾

要充分了解 Cybersource 营收捕手计划，首先有必要回顾反欺诈管理策略的演变过程。

如图 1 所示，反欺诈管理策略在过去 10 年间几经演进，变化明显。最早是专门以阻止欺诈为重点、不计成本的一套规则（反欺诈 1.0），随后发展为更加体现细微差别并主打平衡准确性、运营效率和客户体验的一种方法（反欺诈 2.0），最新成果则是由 Cybersource 制定的一项策略性计划，旨在帮助企业挽回因无卡发卡行遭拒而损失的营收（反欺诈 3.0）。

反欺诈 1.0

立即停止欺诈！
10 年前

反欺诈 2.0

更好的平衡
5 年前

反欺诈 3.0

营收捕手白皮书
现在

图 1| 反欺诈管理策略演变。Cybersource 2020。

反欺诈 1.0

早期欺诈预防引擎采用拒付数据构建，通常存在多达 30 天乃至更长时间的延迟，这意味着其反欺诈策略或模型往往有失准确，而且很快会过时。一些组织因此深受高拒付率困扰，或是被执行监管程序。

久而久之，许多这类企业选择根据高风险甚至中等风险指标自动拒绝更多数量的订单。但是，一味地减少欺诈难免矫枉过正，致使更多合法订单因疑似欺诈而遭拒（即“误报”），造成营收受损，客户体验不佳。相应地，侧重于通过提高通过率来改善面对欺诈时的客户体验的企业最终将更多交易转至人工审核，导致效率下降，运营成本增加。

企业陷入进退维谷境地：缺少简单易行的解决方案用来有效管理欺诈行为；而反欺诈成本、客户满意度和运营成本关联密切，三者之中任一项有变都会波及其他两者。

在早期反欺诈管理当中，企业完全扮演被动角色，阻止欺诈是其主要目标。

反欺诈 2.0

反欺诈管理的新一轮演进源于企业意识到欺诈已成为持续威胁，不宜各个击破，而需要三者统筹兼顾。如下方图 2 所示，这一阶段的挑战是设法在最大限度降低欺诈损失、最大限度增加营收和控制运营成本之间取得适当平衡，继而优化运营。

反欺诈管理团队不得不增聘人手来处理增加的人工审核，此外，不少企业亦大力投资开发内部反欺诈解决方案以应对欺诈行为。这一方面运营成本持续增加，也促使许多企业重新评判他们对反欺诈管理的理解。

反欺诈管理策略的第二阶段要求团队通过确定三项成本的最小组合来优化运营。

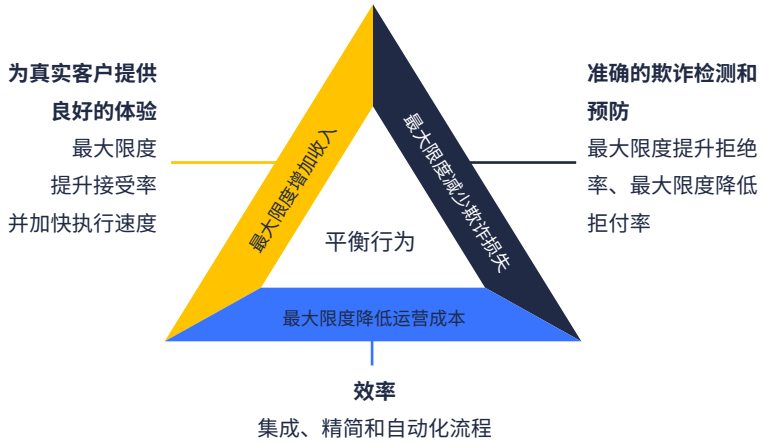

图 2 | 反欺诈管理平衡行为 Cybersource 2020。

反欺诈成本具有动态变化的特性，在反欺诈管理领域历经多年锤炼，许多企业已经积累了足够的反欺诈管理经验，逐渐理解这三种成本的相互作用机制。

在第二阶段，系统和策略趋于成熟，企业得以将注意力集中在更具现实意义的成本管理和改善客户体验上。设备指纹识别和第三方数据验证日益普及，因而更容易直接锁定恶意用户和有组织的欺诈团伙。企业能够在人工审核流程之前更精准地识别和拒绝真正存在高风险的交易，从而减轻人工审核带来的运营负担。

在《平衡掌控大师：如何成为反欺诈管理领导者》（Cybersource 2019 全球电子商务反欺诈管理报告）中，许多企业表示其欺诈损失已在很大程度上得到控制并保持稳定，营收或客户满意度受到的影响得以降至最低限度。[3]

反欺诈 3.0

在任何组织的电子商务策略中，反欺诈管理都将始终是极其重要的一部分，不过，大多数企业（尤其是成熟企业）也已找到自己独特的反欺诈平衡点。

Cybersource 营收捕手计划标志着新时代的开端。作为支付和反欺诈管理领域的行业领导者，我们已联手 Visa 旗下其他企业并协同发卡行和收单行，致力于培育良好的合作关系，因为反欺诈管理的下一步已经超出反欺诈管理本身，其实际意义更在于通过优化授权转换来收复营收失地。

图 3 | Cybersource 风险解决方案副总裁 Andrew Naumann 在“营收捕手”视频中解释了 Cybersource 如何与发卡行和企业合作提高电子商务授权率。观看视频。Cybersource 2020。

3. 问题：对于因疑有欺诈而拒绝的订单，请注明您的订单拒绝率百分比。可能的回答：1. [ ]%；2. 不知道；3. 没有追踪。《平衡掌控大师：如何成为反欺诈管理领导者》（Cybersource 2019 全球电子商务反欺诈管理报告）。

接下来如何?

电子商务营收拥有巨大的增长潜力。到 2023 年，电子商务销售额预计将增至实体销售额的五倍。[4] 如果继续保持目前的增长率，电子商务在未来几年的销售额可能会超过 5.5 万亿美元。[5] 最大限度推动该渠道营收增长至关重要，实现此目标的最佳方法即为缩小无卡 (CNP) 和有卡 (CP) 授权率之间的差距，帮助企业挽回每年可能发生的数十亿美元营收损失。

Cybersource 风险解决方案副总裁 Andrew Naumann 及 Cybersource 其他多位反欺诈管理专家现正与发卡行共同致力于改善其 CNP 拒绝率，目前该数字约为 18%，远高于其 1% 的 CP 交易拒绝率。[6]

这种授权差距仅在美国即相当于每年可能损失数十亿美元的营收。[7]

图 4 | 电子商务授权差距。Cybersource 2020。

4. eMarketer，全球电子商务零售销售，2019 年 5 月。
5. 假设继续保持 15% 的电子商务平均增长率；利用通过 Digital Commerce 360 “2019 年美国电子商务销售额增长 14.9%” 得出的 2010-2019 年同比增长率计算。请参阅：https://www.digitalcommerce360.com/article/us-ecommerce-sales/。估算未考虑新冠疫情对电子商务的影响。
6. VisaNet，2018 年第四季度美国授权率。
7. Cybersource 基于 eMarketer 和 VisaNet 数据计算。

缩小无卡授权差距需要采取突破性方法，Cybersource 在这一方面具备相应的规模和经验。

无卡授权差距
电子商务存在信任问题。

欺诈率在过去几年有小幅增长，电子商务欺诈造成的营收损失中期平均百分比则相对保持稳定。这种稳定性表明企业已找到管理 CNP 欺诈成本的理想平衡点。

尽管如此，发卡行拒绝 CNP 交易的比率仍然过高。就他们而言，CNP 交易还未达到到 CP 交易期间的可用验证数据水平，这意味着 CNP 交易对发卡行的风险通常远高于对企业的风险。因此，发卡行拒绝 CNP 交易的可能性远高于企业 — 如上所述，18% 的电子商务交易遭到拒绝。相较之下，根据 2019 年 Cybersource 全球电子商务反欺诈管理报告的结果，受访者表示因风险评分较高而拒绝的 CNP 订单仅为 3%。[8]

既然如此，授权差距为何是首要问题？电子商务企业对于 CNP 欺诈交易承担大部分责任，发卡行的责任则少之又少。如果证明交易存在欺诈，企业不但会失去这单生意，还必须向发卡行支付拒付费用。当发卡行过于积极地拒绝一个交易时，这些 CNP 企业不仅首当其冲，营收受到更为惨重的影响，还要面临购物车放弃率增加以及忠诚客户流向竞争对手的情况。

发卡行拒绝可能造成隐藏问题

当合法订单遭到发卡行拒绝时，企业可能面临以下情况：

- 失去一单生意
- 将客户拱手让给友商
- 客服团队不堪重负
- 负面口碑传播风险

图 5 | 发卡行拒绝可能带来的负面影响。Cybersource 2020。

8. 人工审核后电子商务订单遭拒百分比（全球）：3%。第 32 页，《平衡掌控大师：如何成为反欺诈管理领导者》（Cybersource 2019 全球电子商务反欺诈管理报告）。

在这些因素直接作用下，大多数电子商务企业能很大程度控制欺诈行为也就不足为奇。现在，企业会在授权之前运行反欺诈解决方案。它们拥有比以往更先进的反欺诈工具和策略，能够获得比过去更多的交易洞察，并利用各种手段拒绝不良交易，这让他们可以更放心地批准更多订单。因此，与发卡行认知当中的接受度相比，企业确认并传送至发卡行的交易（要求付款授权）通常安全性要高得多。

那么，对于企业已经批准的交易，发卡行拒单量为何仍然居高不下？因为许多发卡行仍然只专注于阻止欺诈，而他们拒绝订单依据的是有限的数据点。发卡行无法随时访问企业使用的新交易数据，他们未必完全了解企业的反欺诈管理工具和决策策略已经达到如此准确高效的水平。

企业拒绝的 CNP 交易仅为 3%。[9]

这部分受访者拒绝的交易中有一定百分比实际上属于误报，也即真实客户的合法订单被错误识别为欺诈。尽管企业一直在努力提高检测精度以进一步消除误报，还是会有一些客户受到负面影响。完美无缺的反欺诈解决方案显然不存在；即使采用稳健的反欺诈管理策略，大量企业仍有 0.7% 的平均拒付率。[10] 完美无缺的反欺诈解决方案显然不存在。

9. 人工审核后电子商务订单遭拒百分比（全球）：3%。第 32 页，Cybersource 报告，同上。
10. 欺诈拒付率，占年度电子商务营收的百分比（北美、中东和非洲、欧洲）：0.7%。第 32 页，Cybersource 报告，同上。

从这一角度来看，发卡行的做法便不难理解。CP 交易提供通过 EMV 芯片动态生成的标识符，以及与持卡人的面对面互动、签名和其他识别数据点，有助于发卡行更放心地处理这些交易。相比之下，就发卡行而言，CNP 交易似乎更加匿名化，恶意行为者可能会采取多种策略来规避风险信号。因此存在一定风险，不过程度较发卡行预期要低。

如图 4 所示，即使不考虑信用能力问题，每年仍有 18% 的 CNP 交易遭拒，仅在美国即会造成数十亿美元的损失，而随着全球电子商务市场不断扩大，这一数字只会继续增长。[11]

需要指出的是，发卡行将对交易进行独立评估，所采取的不同标准也会影响到授权决策。诚然，拒绝率因发卡行、垂直行业和地区而异，尽管如此，这些拒绝仍然意味着企业营收严重受创，因而支付生态系统中的所有参与者必须共同努力，使这一数字尽可能接近 3% 的企业拒绝率。[12]

这些拒绝对客户的影响更不必说，优质客户流失会令企业付出高昂代价。当今市场环境竞争激烈，消费者如果平白无故被拒绝交易，很可能立即点击鼠标一键转投友商怀抱，企业不止损失一单交易，日后也很难再让消费者回心转意。

反欺诈经理和支付经理的角色开始略有重合，因为发卡行拒绝本质上被视为外部误报。但不同于内部误报，解决此问题的方案较为有限。

营收捕手计划应运而生...

无卡交易数据点

- 缺少 ID 验证
- 缺少 EMV 代码
- 缺少签名

有卡交易数据点

- 卡片实际存在
- 可使用其他形式的 ID 验证身份
- EMV 芯片生成唯一交易代码
- 可获取签名以供稍后验证

图 6 | 与无卡交易相比，发卡行掌握的无卡交易数据相对有限。Cybersource 2020。

11. Cybersource 基于 eMarketer 和 VisaNet 数据计算。
12. 人工审核后电子商务订单遭拒百分比（全球）：3%。第 32 页，《平衡掌控大师：如何成为反欺诈管理领导者》（Cybersource 2019 全球电子商务反欺诈管理报告）。

营收捕手五项计划
构建反欺诈管理的未来

Cybersource 挽回营收损失的策略有赖于大多数电子商务企业已将其欺诈率控制在可控范围内。

得益于公司长期以来在电子商务支付领域领先一步，加之身为 Visa 全资子公司，Cybersource 拥有得天独厚的优势，能够从根本上转变企业和发卡银行互动方式，乃至改变支付处理方式，进而帮助提高 CNP 授权率。

为了将我们的营收捕手愿景变为现实，Cybersource 反欺诈管理和支付专家制定了五项关键计划，旨在助力企业迈出电子商务营业额增长的下一步。增强欺诈管理工具和分析功能、提高授权率可见性并降低交易处理阻力，有利于企业获取营收、发卡行收取手续费以及买家收到产品。

1. 降低拒付率

发卡行授权率与企业拒付率挂钩。如果企业欺诈率较高，发卡行在授权交易时会相对谨慎。当企业降低其拒付率时，也就相当于向发卡行发出信号，表明他们已改善反欺诈管理流程。发卡行处理这些企业的交易时会相应地放宽要求，从而提高企业授权率。

Decision Manager 的高级机器学习模型可以帮助企业评估其历史交易数据，进而发现相应的模式、确定新策略并做出更好的支付决策。Decision Manager 具备强大而灵活的规则管理功能，可为企业提供创建一组精准规则所需的控制，这将帮助他们降低拒付率，同时谨慎做出调整，以适应组织扩大销量和提升客户体验的目标。

2. 授权率报告

反欺诈团队通常埋首于海量数据。从规则完善到人工审核，再到确定是否提出拒付，大量决策由交易信息驱动。然而，多数反欺诈经理目前对于其发卡行授权状态一无所知。许多企业要么并未意识到存在问题，要么认为自身没有能力在组织以外推动变革。

缺少初始基准，企业几乎不可能第一时间确定是否存在超出范围的授权拒绝问题，或者无法有效衡量他们是否在缩小差距方面取得进展。Cybersource 首先帮助企业了解和掌握其发卡行授权率。除了跟踪过往内部绩效之外，Cybersource 还帮助企业将自身绩效比照类似行业和垂直市场的其他组织进行基准测试。

发卡行拒绝后续步骤

企业应围绕这些关键点发展纵深知识体系和方案

- 了解其拒绝率
- 分析交易遭拒原因
- 对人工审核后发生的拒绝予以审查；根据需要重新评估工具和流程
- 通过授权原因代码进行拒绝分析；找出峰值及其他异常

3. 授权之前预先筛查交易

企业日益认识到在提出授权请求前将大部分或全部反欺诈筛查移至上游的价值。

在授权之前将交易提交至 Decision Manager，这种操作顺序更改可能会导致交易费用略有增加，但下游优势也会更加凸显。Decision Manager 的预筛查流程可利用机器学习和企业自有反欺诈规则，先行净化要向发卡行提交的交易，以便提高交易转化率。

这种方法让企业得以在提交授权之前过滤并拒绝具有极高风险的交易，或是源自已知反欺诈数据点的交易，因而可将一组欺诈行为更加踪迹难寻的交易传送至发卡行。

这些净化后的交易有助于降低发卡行拒绝率并减轻运营负担，同时有助于推动企业历史欺诈率的改善。一段时间过后，发卡行对企业的信任度将有所提升，授权通过率也会随之好转。提高授权率以挽回营收损失作为最终目标，考虑对营业额的积极影响，运营成本增加可谓物超所值。

图 7 | 将反欺诈筛查移至上游，以在提出授权请求的同时向发卡行提供其他信息。Cybersource 2020。

回顾既往欺诈交易策略

企业以往会在提交交易进行反欺诈筛查之前先将交易提交给发卡行，以确保帐户有效且资金可用。

这么做原因有二：

首先，企业能够获取发卡行响应工具（如地址验证服务和卡片验证码）的结果，这样通常可为其决策过程加码。

其次，能够减少提交至第三方反欺诈解决方案进行评估的交易量，从而帮助降低运营成本。

4. 优化工具配置

组织可以使用多种工具，包括人工审核、二级处理、身份验证和智能路由。那么，手段如何选择，何时介入，使用这些工具应当遵照何种顺序？Decision Manager 领先的分析和报告有助于优化这些工具，使 Cybersource 能够创建自行调节的反馈回路。

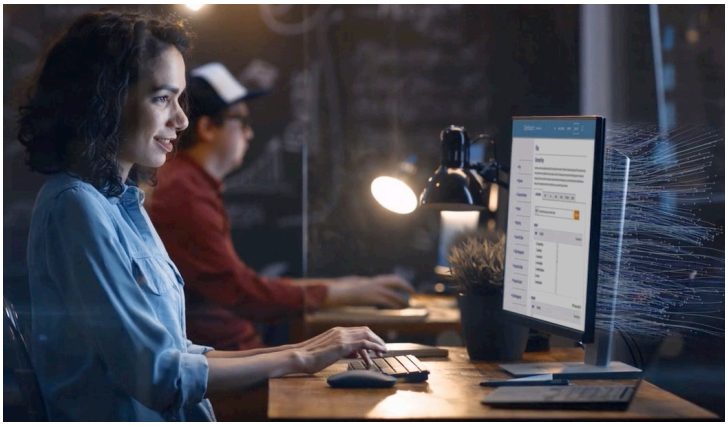

图 8 | Cybersource Decision Manager 使用机器学习持续改进其反欺诈功能。Cybersource 2020。

通过使用机器学习统筹安排支付收单受理和交易路由等操作的自动规则校准，Cybersource Decision Manager 可减轻反欺诈管理团队的决策负担，使他们能够更好地专注于转至人工审核的案例。

不断整合新的交易历史记录和各种决策排列分析将优化工具配置，并有助于最大限度提高完成率。

5. 通过自动身份验证维护客户体验

Cybersource 正在与受欧盟支付服务修订法案第二版 (PSD2) 指令强客户身份验证 (SCA) 影响的客户合作。Cybersource 3DS 验证解决方案将帮助自动进行身份验证并最大限度对 SD2 SCA 指令应用豁免，以期降低客户付款流程阻力。

通过 Decision Manager 提供的 3DS 验证可令企业更好地控制其客户支付体验，同时还提供最新一代 Cybersource EMV® 3D 验证解决方案[13]（支持 SCA 要求）的所有优势，包括欺诈责任转移和降低手续费用。

实施此工具使企业可以决定何时请求 3DS 验证保护，有助于确保其优质客户享受流畅的结账体验，同时支持遵守最新 PSD2 SCA 指令要求。

为防止授权率下降，有必要结合使用 Cybersource 3DS 验证解决方案，依托其强大的反欺诈筛查策略及豁免优化服务。

13. EMV® 是在美国和其他国家/地区的注册商标，以及其他区域的非注册商标。EMV 商标归 EMVCo, LLC 所有。

强客户身份验证 (SCA) 简介

欧盟 PSD2 SCA 指令要求对收单行和发卡行均位于欧洲经济区、英国或直布罗陀的某些电子商务支付交易执行严格的客户身份验证。该法案 SCA 指令于 2019 年 9 月 14 日生效，而预计于 2021 年开始正式施行。[14]

如有 SCA 要求，付款方需通过至少两个因素进行身份验证，每个因素必须来自不同类别：

- ✔ **付款方掌握的信息** — PIN、密码等
- ✔ **付款方可用的工具** — 口令生成工具、预先注册的移动设备等
- ✔ **付款方的身份证明** — 指纹、语音匹配等

如需了解有关 PSD2 的更多信息，请访问：
www.Cybersource.com/psd2

如需了解有关 SCA 的更多信息，请访问：
www.Cybersource.com/en-gb/psd2-sca

在该地区销售的电子商务企业需要能够支持 SCA，否则可能发生遭拒交易增加。

SCA 的优势

1. SCA 令持卡人更加安心无忧。
    a. 加强版安全措施，例如发卡行可使用双因素验证对持卡人进行身份验证，验证通过将可提高持卡人信任度。
2. SCA 为创新提供动力。
    a. SCA 助力 EMV 3DS 2 协议推行。与 3DS 1 相比，EMV 3DS 2 协议使企业与发卡行共享的数据增加 10 倍，进一步完善发卡行验证策略并提升决策能力。

14 EBA 意见，2019 年 10 月 16 日发布。请参阅：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

未来创新

营收捕手计划将继续发展完善，寻求能够帮助弥合 CNP 授权差距的新途径。本节探讨未来我们会在下一阶段开发中主推的几项新功能。

1. 智能路由工具

智能支付路由流程通过分析历史交易标准，将不同类型的交易与适当的收单行进行匹配，帮助企业进一步提高授权通过几率，继而最大限度提高授权率。

除了采用多重标准，这项功能还将考虑美元金额、是否为跨境交易以及实际发卡行，随后路由至后端的相应处理器。

Decision Manager 将来能支持基于 API 的智能路由，并在任意 API 字段中配置规则以正确路由交易。此外，Decision Manager 还将提供基于聚合参数（美元金额、交易量等）路由交易记录的功能。

可针对单笔订单进行配置

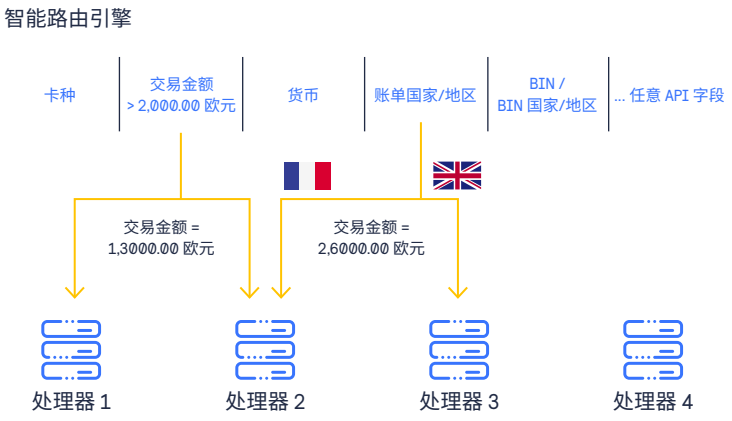

图 9 | 可针对单笔订单进行配置。Cybersource 2020

智能支付路由可将金额、跨境账单、发卡行、任意 API 字段及各种聚合参数纳入考量，然后将交易路由至后端的相应处理器。

针对交易量或金额执行聚合

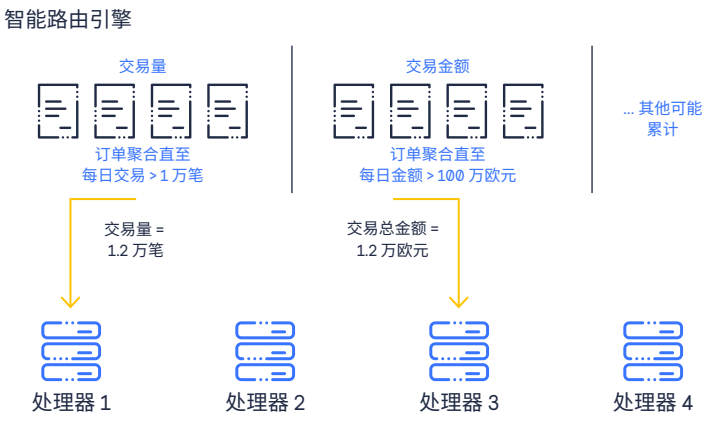

图 10 | 可针对单笔订单进行配置。Cybersource 2020

2. 与 Verifi 合作实施拒付管理

Cybersource 将在 Decision Manager 中集成 Verifi 的 Order Insight。Order Insight 在客户查询的第一点向发卡行和客户提供增强的订单数据，以帮助防止争议。Order Insight 可节约发卡行时间、消除客户困惑并帮助企业减少争议和拒付，这也有助于防止品牌受损和客户流失。最重要的是，该工具可将原本会发生的拒付转化为合法交易。

3. 授权之前与发卡行共享风险评分

打破惯例，在授权之前先运行反欺诈规则以便预筛交易，可令发卡行在接受授权请求时更有把握。此外我们也在研究新功能，允许企业在提出授权请求的同时共享部分此类预筛查结果数据（例如风险评分等），为发卡行进行风险评估提供有益的补充。当交易请求中能够包含这些额外数据点，显示“此交易已由 Decision Manager 预先筛查”时，发卡行即了解这类标记的交易带来的风险较小。

借助营收捕手进一步提高可见度和增加信任度

通过在大多数电子商务市场采用有效的反欺诈策略，并将欺诈损失稳定在较低的最佳百分比，企业最终能够集中精力通过营收捕手计划最大限度增加营业额。反欺诈 3.0 时代将着重降低授权拒绝率、提高可见度以及在授权前更好地了解无卡交易。

Cybersource 致力于与 Visa、企业、发卡行和收单行合作，在支付实体之间建立更顺畅、更全面的沟通，以提高对 CNP 交易的可见性，同时降低各方决策阻力和总体风险。

Cybersource 营收捕手计划最基本的目标是提高发卡行授权率、提升客户满意度及挽回营收损失。Cybersource 和 Visa 具备相称的经验、规模和人脉，将当仁不让引领这一领域的变革。能成为支付和反欺诈管理的行业领导者，Cybersource 深感自豪。

本白皮书包括Cybersource正在持续开发的程序以及持续完善的概念和细节。Cybersource可自行决定修改、更新或取消任何Cybersource特性、功能、实现过程、品牌推广和时间安排。程序和功能普遍适用的时间范围还受到 Cybersource 无法控制的多项因素制约，包括但不限于由发卡行、收单行、商家和移动设备制造商部署必要的基础架构。此外，某些现有功能并非在所有国家/地区均适用。参与计划和服务须遵守 Cybersource 在计划参与协议及相关文档中的条款和条件；要求收单行参与、批准或保荐商家登记。

本白皮书包含符合 1995 年《美国私人证券诉讼改革法案》规定范围的前瞻性陈述。这些陈述通常包含“计划”、“目标”、“可用”、“可能”、“将要”等字样或其他有关未来的类似表述。此类前瞻性陈述的示例可能包括但不限于我们就路线图、公司战略及产品目标、计划和宗旨所作的陈述。就其性质而言，前瞻性陈述：(i) 仅反映截至陈述作出当日的情况；(ii) 既不是历史事实陈述，也并非对未来业绩的保证；(iii) 受到难以预测或量化的风险、不确定性、假设和情况变化的影响。因此，由于存在一系列因素，实际结果可能与这些前瞻性陈述出入较大甚至相悖，包括：法律和/或监管变更影响；开发周期中断和/或问题；发展重点修改；以及 Cybersource 母公司 Visa Inc. 在最新 Form 10-K 年报和我们的最新 Form 10-Q 季报中“风险因素”(Risk Factors) 标题下所讨论的其他因素。不应过分依赖此类陈述。除非法律要求如此，否则我们无意出于新信息或未来发展或其他原因而更新或修订任何前瞻性陈述。

比较结果、统计数据、研究和建议事项均依照“原样”呈现，仅供参考之用，不得作为经营、营销、法律、技术、税务、财务或其他领域的依据。Cybersource 既不对本文件中信息的完整性或准确性作出任何保证或陈述，也不对因依赖此类信息而可能导致的任何后果承担任何责任。本文所含信息并非作为法律建议，我们鼓励读者在需要此类建议时征求合格法律专业人士的意见。

所有营收捕手计划* 均通过 Cybersource 企业反欺诈管理解决方案 Decision Manager 实施。

如需详细了解 Decision Manager 以及贵组织如何实施营收捕手领域的行业领先方法来优化授权率，请立即访问 Cybersource.com 与 Cybersource 联系。

*Cybersource 可自行决定更改或取消所有计划。

cybersource
A Visa Solution