电子商务欺诈全解析

洞悉和管理在线欺诈的实用指南

cybersource
A Visa Solution

目录

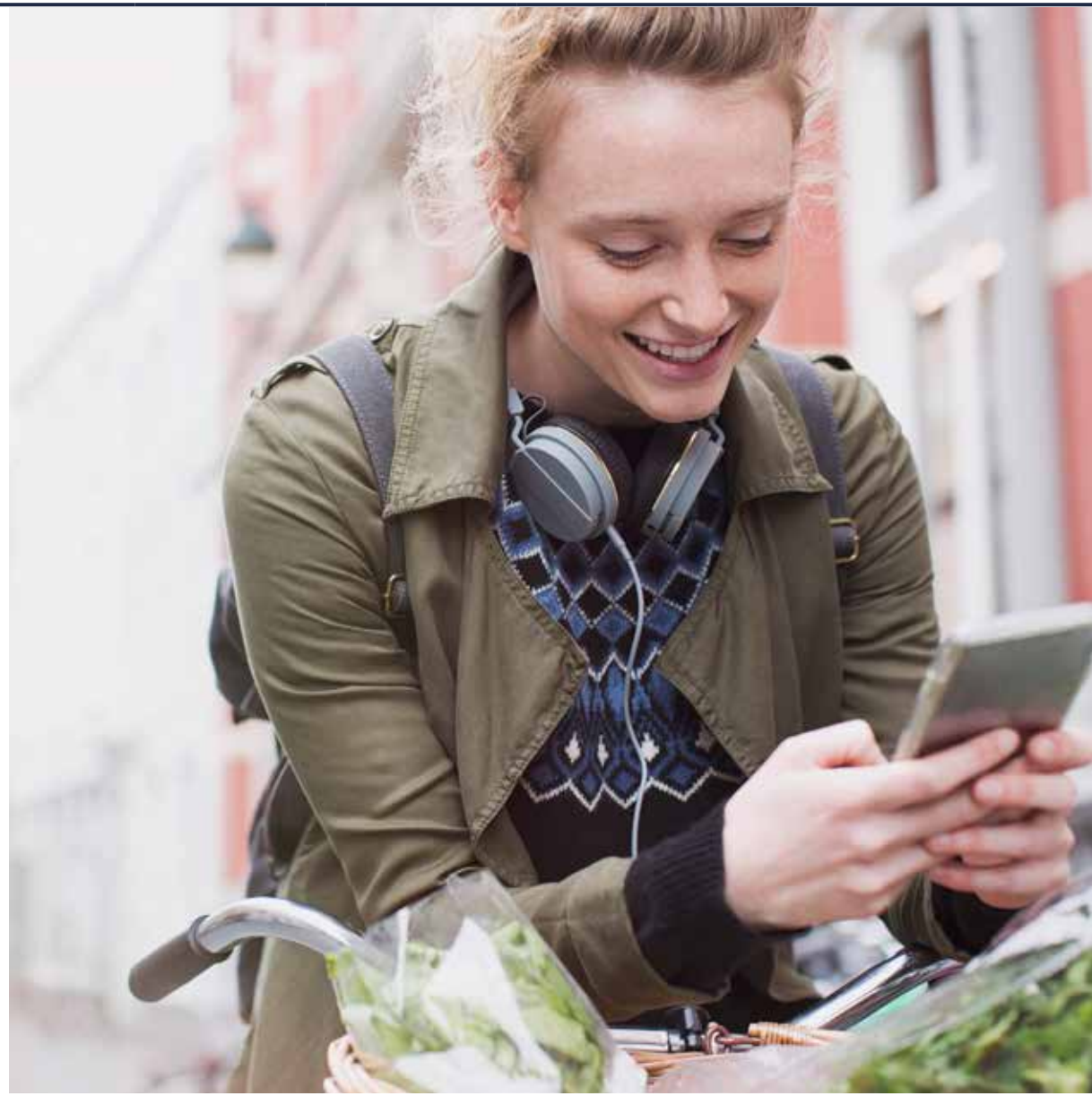
为何要编写本指南？

提供对于反欺诈管理的新洞见协助您实现业务的快速发展

世界众多的电子商务巨头均选择通过 Cybersource 来管理风险并减少欺诈。我们致力于帮助这些企业制定有效策略并部署最佳服务组合，从而有效管理跨渠道和跨境欺诈行为。

贵企业可能需要新的洞见，从而能够在短时间内快速完成从内部程序到 Cybersource 解决方案的迁移、从其他反欺诈服务的过渡，或者对反欺诈部门新员工的培训。又或者，您即将要开展新业务，打算采用数字化支付方式，为此想要更深入透彻地理解电子商务反欺诈管理中涉及的一些关键概念和策略。

本指南涵盖开展有效的反欺诈管理所需的一切基础知识，能够帮助您了解如何才能最大限度增加收入、减少欺诈损失和降低运营成本。



电子商务欺诈有哪些形式？

从账户冒用到灰色市场销售，欺诈手段多样，表现形式不一

电子商务欺诈会以不同的形式出现。是一种由个人（或有组织的犯罪集团）通过在线商店所实施的非法行为。由此所带来的后果包括未经授权或欺诈性交易、商品被盗或错误的退款请求。有关常见电子商务欺诈类型的更多信息，请详见下文。

账户冒用问题日趋严重

59% 的 Cybersource 2019 全球电子商务反欺诈管理报告的调查受访者预测，账户冒用攻击会在接下来 12 个月增多。[1]

[1] Cybersource，《平衡掌控大师：如何成为反欺诈管理领导者》（2019 全球电子商务反欺诈管理报告）。就其性质而言，前瞻性陈述会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。

电子商务欺诈概观

认识常见的电子商务欺诈类型

1 账户冒用

欺诈者利用所盗取的登录凭证控制电子商务站点、银行站点或支付解决方案上的他人账户。欺诈者可能会修改个人信息，或者利用账户内的支付详细信息进行购买。

2 线上购买，门店取货

欺诈者利用窃取的信息在线进行购买，然后在零售商检测到其欺诈行为之前到实体店提取商品。

3 “毫无破绽”的欺诈

欺诈者利用盗取的信用卡进行在线购买，输入足够的正确持卡人信息，让交易看起来真实可信，最终成功骗过企业的安全检查。

4 卡测试

欺诈者会借助自动机器人利用盗取的信用卡号进行大量的小额交易。通过这些测试，确定出可以将哪些卡用于其他更高价值的欺诈交易，哪些应该弃之不用。

5 第一人称欺诈

客户用自己的支付卡购买商品，然后声称购买未经授权或商品未送达，以此来索要赔偿。企业为此而向客户赔付费用，客户其实相当于免费获得了商品。（也称为*友好欺诈*）。

6 退款或退货欺诈

欺诈者利用盗取的凭证在线购买商品，然后前往实体店请求退款，由于缺少有效的商店收据，多数情况下会获得商店礼品卡。

7 重新运送欺诈

欺诈者利用盗取的支付详细信息购买商品。然后，欺诈者联系托运人，请求将商品配送到新的地址，或者付钱给一些人（即所谓的货运代理人）来冒充收货人。货运代理人将商品重新配送给欺诈者或运送至其他地点进行转售。

8 灰色市场欺诈

欺诈者利用盗取的信用卡购买商品，然后将其转售到未经授权的市场或地区，或将其打折出售。（也称为*经销商欺诈*。）

9 忠诚度奖励计划欺诈

欺诈者在未经授权的情况下访问与商户所提供的忠诚度奖励计划相关联的账户。

电子商务欺诈为何如此普遍？

欺诈向线上转移

美国实卡当面交易的欺诈率减少了

82%[3]

然而，美国无卡线上交易的欺诈率上升了

33%[4]

易于获取信息的优势和愈加严密的实体店安防措施促使欺诈者将欺诈转移到线上

到 2023 年，全球零售商和电子商务企业在反欺诈管理解决方案上的总支出预计将达到 90 亿欧元。

电子商务欺诈的高发率与以下两个主要因素有关：

易于获取信息

1. 欺诈者只需要花很少的钱就能很轻易地买到因数据泄露和黑客攻击而被盗取的支付和身份信息。[2]

严密的实体店反欺诈措施

2. 利用 EMV（Europay、Mastercard 和 Visa）技术将计算机芯片嵌入信用卡中，以实现持卡人数据的安全存储，也被称为“Chip-and-Pin（芯片密码）”技术。鉴于这一情况的出现，越来越多的不法分子开始将阵地转移至线上

[2] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf
[3] Visa，芯片卡统计数据，2018 年 11 月 27 日，https://usa.visa.com/visa-everywhere/blog.entry.html/2018/11/27/chip_technology_has-u1kX.html
[4] Aite，“3D 验证 2.0：发卡机构的主要注意事项”，2018 年 2 月 21 日，https://www.aitegroup.com/report/3-d-secure-20-keyconsiderations-card-issuers
就其性质而言，前瞻性陈述会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。

新冠肺炎疫情的不期而至再次触发欺诈格局的调整

为适应出现的“新常态”，比如订单量的快速下降和激增，新政府政策的频频出台，以及劳动力的不足或频繁更换，企业不得不进行相应的调整，这在无形之中可能会产生新的漏洞，为欺诈者提供更多的可乘之机。

欺诈者无疑会加紧测试商户的账户，以找出哪些存在最大的漏洞。为确保业务和客户的安全，您需要积极采取创新性措施，以洞悉哪些很可能会成为欺诈者的目标并抢先一步加以防范。

趋势

当经济陷入困境时，欺诈者深知，面对这种情况，一些企业会倾向于消除或调整任何已知的障碍以促进销售，这会更有利于他们乘虚而入。

人工欺诈审查团队可能会面临人手不足的问题，可能会影响到接受/拒绝模型或让一些规则变得更加宽松。

卡测试问题最为凸显，呈大幅上升趋势。在此类攻击中，欺诈者对僵尸网络进行编程，使其能够在商户站点上运行数千笔交易，以此来“测试”卡详细信息的有效性。这致使许多商户的授权率受到影响。

机器学习和人工智能模型在构建时并未考虑新冠肺炎疫情因素，致使疫情期间出现很多误报，这意味着您可能会将很多真实订单拒之门外。虽然这些模型最终有可能会根据新冠肺炎疫情下的欺诈趋势重新进行调整。但这无疑需要花费时间来完成，而这种等待可能会让您蒙受无法承受的损失。

对策

您需要在不影响当前客户支付体验的情况下实现对新风险策略的快速评估。借助 Decision Manager Replay，您可以根据历史交易数据对不同的“假设分析”反欺诈策略实时进行测试。这让您能够在将规则变更投入生产之前就其对于风险管理策略的影响做出快速评估。从而更快地找出最佳规则变更并将其应用于实际环境中。

如果您在评估反欺诈管理策略的过程中需要更多帮助，**我们的风险管理分析师会不遗余力为您提供洞见**和专业知识，与您一起共度时艰。他们的工作跨越多个行业和地区，熟知所有最新的策略和方法。

重新考量目前所用的方式，以轻松化解变幻莫测的欺诈招式

电子商务持续发展，电子商务欺诈则是如影随形。为了识别和防范层出不穷的欺诈者策略，采用现代化的反欺诈管理系统比以往任何时候都更为重要，该系统使用先进的计算机模型，并从不断更新的全球交易数据中提取信息。

趋势

自 20 世纪 90 年代中期以来，电子商务得到迅猛发展。如今的消费者会使用各种设备，并通过多种支付方式在线购买五花八门的产品和服务。

电子商务企业逐渐走向全渠道经营模式。致力于跨电子商务和传统渠道提供无缝的客户体验。一些企业让客户能够在线浏览和购买也许并无库存或者在实体店中购买不到的商品。（也称为*无限货架*。）

对策

电子商务欺诈也日渐频繁。欺诈者正在不断筹划新的手段和策略，以期能够在最新的电子商务销售渠道和支付方式中找出可乘之机。

欺诈者给人们的印象也在逐渐改变。电子商务欺诈不再局限于个人或小型团队的行为。如今的欺诈已演化为一个特殊行业，涉及众多的国内和国际犯罪团伙以及众多的复杂技术。[5]那么，这里的“如今”所指何意？Cybersource 已对国内和国际欺诈犯罪团伙做了至少三年的并行展示。[6]

[5] 美国联邦调查局，“跨国有组织犯罪”，https://www.fbi.gov/investigate/organized-crime
[6] Cybersource 通过欺诈演变时间轴展示了国内和国际欺诈犯罪团伙的发展情况。

反欺诈管理具有哪些帮助性作用？

反欺诈管理有助于减少财务损失并降低声誉受损的风险

[7] Cybersource 2019 年 5 月计算数据，基于 eMarketer，全球电子商务和移动商务，2019 年 5 月（数字已四舍五入）；以及 Cybersource 于 2018 年 10 月进行的 GfK 研究。就其性质而言，前瞻性陈述会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。

确保拒付处于可控状态

当客户就其银行卡对账单上的商品向发卡行提出争议并被成功受理后，发卡行将会撤回对企业账户的付款或执行拒付。与欺诈有关的争议分为两类。

1. **第三方欺诈：**欺诈者利用持卡人信息进行未经授权的购买。持卡人向其发卡银行提出争议。当持卡人的对账单上出现欺诈交易时，可能需要 30 天或更长的时间才能注意到该欺诈交易。
2. **第一人称欺诈：**持卡人对正当的信用卡收费提出争议，以避免为商品付款。（也称为友好欺诈）。

Visa 和 Mastercard 等支付网络均严格规定了可接受的拒付率上限。拒付率超过银行卡网络所规定上限的零售商将被置于拒付监视列表中。
此类零售商可能还会：

- ✓ **支付更高的订单处理费**，导致所得利润减小
- ✓ **丧失对抗拒付的能力**，需等到拒付率降低之后方可恢复此能力
- ✓ **被置于拒付监控程序中**，并会因信用卡联盟试图帮助其降低拒付率而需要支付更多费用

与此相反，拒付率不断优化则是有效反欺诈管理的标志。Cybersource 2019 全球电子商务反欺诈管理报告发现，在反欺诈管理方面表现突出的企业，其平均自述拒付率比其他企业低了四倍之多。[8]

通过优化拒付率，您能够最大限度减少欺诈损失，同时又不会导致良好客户的流失。

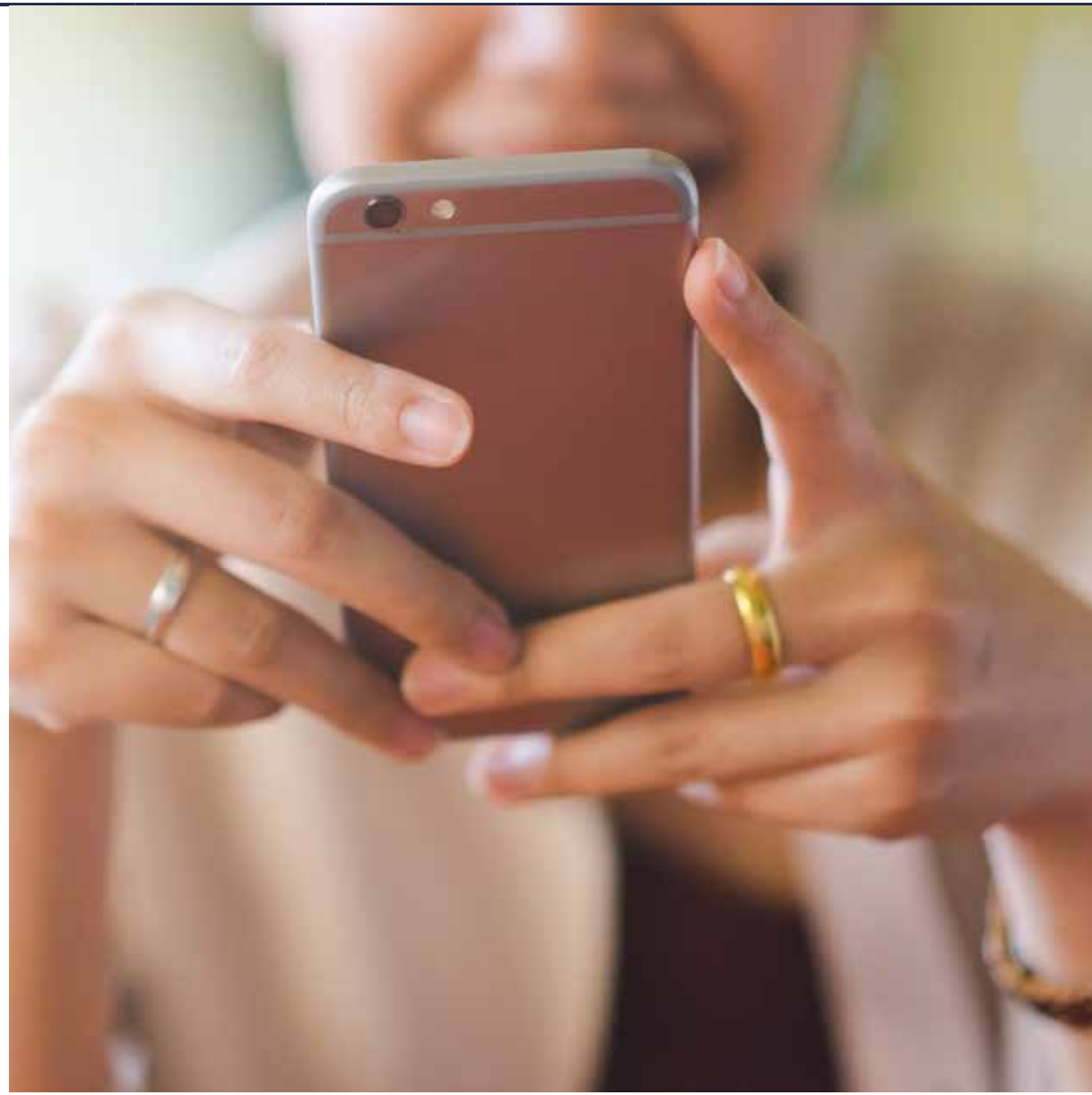
[8] Cybersource，《平衡掌控大师：如何成为反欺诈管理领导者》（2019 全球电子商务反欺诈管理报告）

如何借助在线支付流程有力打击欺诈？

了解在线支付运作原理有助于更好地规划反欺诈管理策略

在线支付涉及多个环节，只有协同运作才能确保提供无摩擦的客户体验，并成功筛查出欺诈性交易。
例如：

1. **一位客户点击了“立即购买”**
2. **公司的支付网关收集交易**和订单信息，并将信息传递给支付处理机构。
3. **支付处理机构与客户的发卡行进行核实以确认：**
   - ✓ 所用的银行卡有效
   - ✓ 资金可用于购买
   - ✓ 交易与地址验证服务 (AVS) 和卡验证值 (CVV) 响应匹配
4. **与发卡行确认后，支付处理机构将：**
   - ✓ 对资金进行授权保留（以便零售商能够在转账之前对订单进行审核），或者
   - ✓ 安排资金以完成向收单行中企业账户的转账



反欺诈管理面临哪些主要挑战？

主要挑战包括无缝客户体验、跨渠道销售和合规性[9]

对于许多企业而言，反欺诈管理中的挑战不仅限于防范欺诈者。他们需要在多个目标（最大限度增加收入、最大限度减少欺诈损失和最大限度降低运营成本）之间实现最佳平衡。同时力求打造一种全新的跨渠道客户体验。并且确保符合各项新出台的法规。

[9] Cybersource，《平衡掌控大师：如何成为反欺诈管理领导者》（2019 全球电子商务反欺诈管理报告）

实现收入、欺诈损失和运营成本之间的平衡

有效的反欺诈管理可以让您在打击欺诈和提高运营效率的同时打造出色的客户体验，从而成功实现增收。

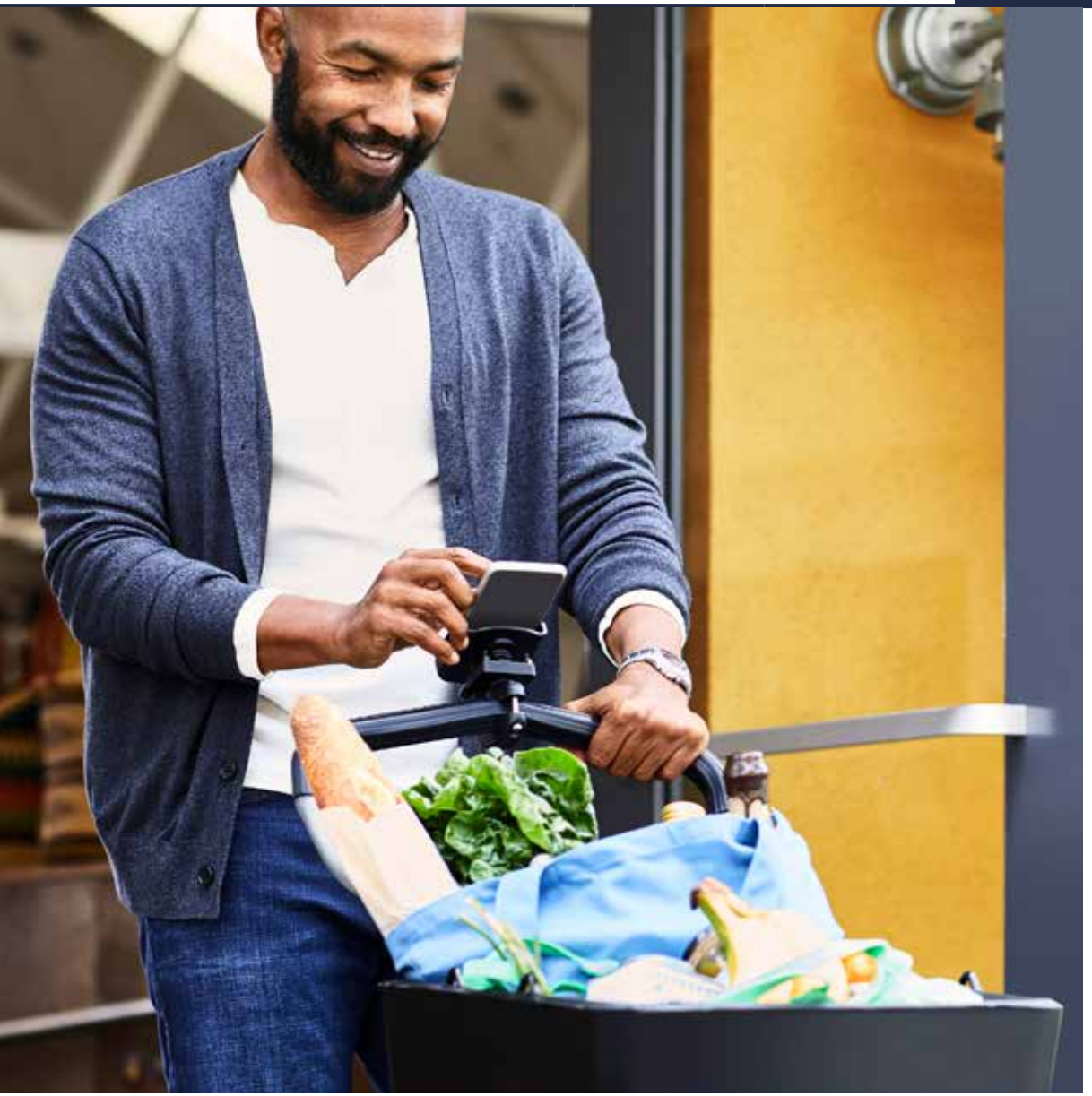
最大限度增加收入：为提供无缝客户体验，让良好客户始终舒心满意，应确保交易流程的顺畅、快速和无摩擦。确保反欺诈措施不会减慢交易速度，错误地拒绝真实订单（误报）或给客户带来不便。令人沮丧的交易可能会将您的客户拱手送给竞争对手。

最大限度减少欺诈损失：为了能够检测出欺诈性订单，最大限度防范各类欺诈行为，您需要具备识别新兴攻击并给予回击的能力。
但要做到这些并非易事。

最大限度降低运营成本：无论采用何种反欺诈管理解决方案，都需要简化流程并实现流程自动化，以控制运营成本，并将欺诈审核员人数保持在较低水平。

2019 年，电子商务企业普遍认为跟上不断演变的欺诈趋势是反欺诈管理中需要面临的一项主要挑战。[10]

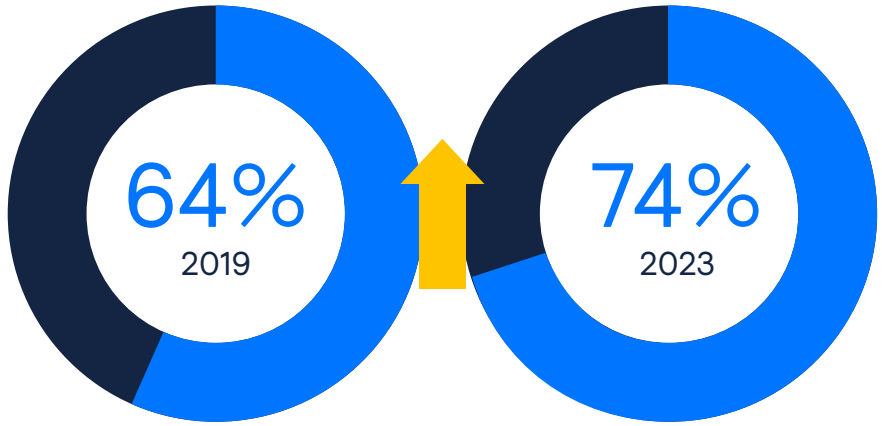
[10] Cybersource，《平衡掌控大师：如何成为反欺诈管理领导者》（2019 全球电子商务反欺诈管理报告）



采取跨渠道策略

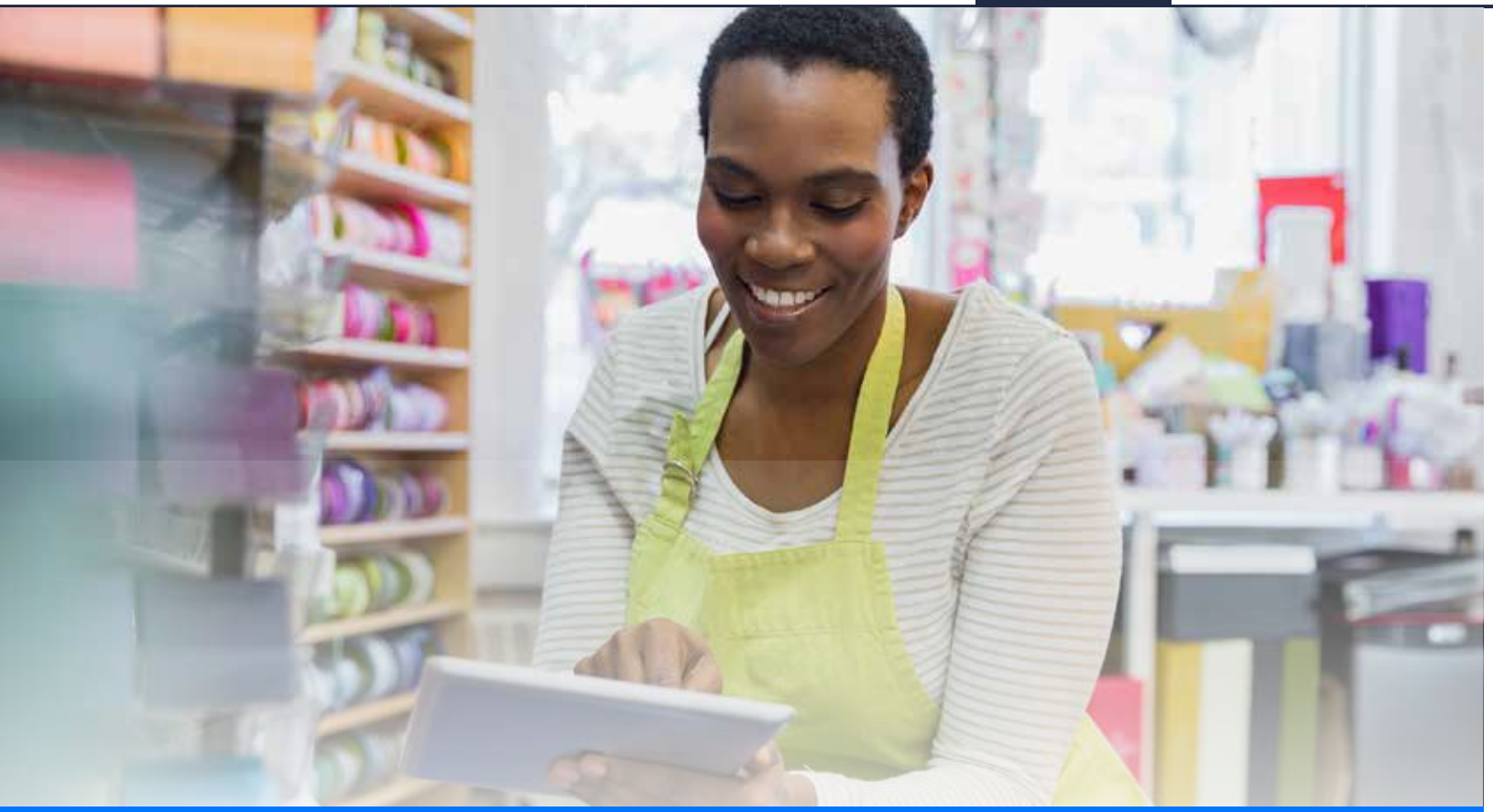
在世界日益多样化，消费者购物方式多种多样的大背景下，关注真实客户的行为可以带来诸多好处。除了实体店购物、电话购物和平邮购物，消费者开始越来越多地在智能手机和平板电脑上通过移动应用进行购物，以及通过笔记本电脑和台式机登录网站进行购物。在许多情况下，消费者会多渠道并用，比如在线下单，然后到店取货。

人们正越来越多地使用移动支付



到 2023 年，移动支付在全球所有电子商务支付方式中的占比预计将从 2019 年的 64% 升高至 74%。[11]

[11] eMarketer，全球电子商务和移动商务，2019 年 5 月（数字已四舍五入）。就其性质而言，前瞻性陈述会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。



全渠道成为首要任务

94%[12] 的零售商表示，全渠道服务策略是公司的首要任务之一。

[12] Forrester 数据：2017 年至 2022 年受到数位影响的零售销售预测（美国）

利用跨渠道反欺诈管理增进对真实行为的了解

欺诈者试图向不同渠道渗透的事实足以说明为反欺诈管理制定跨渠道策略的必要性。跨渠道策略还有助于您增进对于真实行为的了解。如果不考虑各渠道购买行为之间的差异性，就有可能会把活跃于多个渠道的客户误当作欺诈者。这意味着您应该具备以下能力：

1. **自动筛查订单**，找出特定渠道和特定设备中的欺诈行为
2. **轻松识别出真实的客户**（和订单），并在所有渠道中为消费者提供无缝的结账体验

符合新兴法规

欧洲银行业管理局在支付服务指令 2 (PSD2) 中增设了新的监管技术标准。这些安全标准中很重要的一部分内容便是对于强客户身份验证 (SCA) 的规定。当前，仅当收单行和发卡行均位于欧洲经济区 (EEA)、英国和直布罗陀时，才需要遵守 SCA 的规定。PSD2 要求将 SCA 应用于某些电子支付，包括 EEA 内的近场支付、远程支付和移动支付。

根据 SCA 的规定，消费者需要通过以下三种方式中的两种来验证其身份：展示自己的身体特征（使用生物识别）；他们所独有的东西（SIM 卡、预注册的移动设备或令牌生成器）；以及他们所知道的信息（PIN 或密码）。商户应确保做好随时支持 SCA 的准备，以防止发卡行拒绝交易。

PSD2 SCA 可能会影响在欧洲经济区 (EEA)、英国和直布罗陀开展在线业务的任何组织，以及推进在线支付的银行、金融科技和其他金融服务公司。

在某些情况下，比如交易风险较低、交易价值较低、交易由商户发起，为了能够给客户带来无摩擦的支付体验，可以采用 SCA 指令与有限豁免相结合的形式。

处在监管范围内的发卡行和收单行有责任应用 SCA 和适当的豁免，从而实现客户便利性和减少欺诈之间的最佳平衡。

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

强客户身份验证 (SCA) 要求以三种不同方式中的至少两种来验证消费者的身份

反欺诈管理的最佳方式是什么？

利用多层次方法力求达到最佳平衡

利用多层次方法（采用多种工具和技术）有助于您快速准确地区分出真实订单和欺诈订单。

面对当今欺诈者复杂多变的手段，单凭一种工具无法确保企业的安全无虞。专注于单一威胁或能力的单点解决方案无法防范全部的欺诈活动。此外，如果只是一味的想要减少直接损失，将很难实现各个目标（减少欺诈、提供优质客户体验和实现增收）之间的最佳平衡。

通过采用战略性的分层方式，同时使用多种反欺诈管理工具，以不同方式来监测欺诈，组织能够更加有效地防御各种针对越来越多销售渠道的攻击。企业需要在实施网络级别保护的同时加大培训力度，以帮助团队更好地理解结账流程最佳实践以及如何检测和缓解社会工程。为了力求让业务达到最佳平衡，您还需要整合多个解决方案，以增大批准量并最大程度减少误报，最终实现客户体验最优化和收入最大化。

将多种工具和技术纳入多层次方法

利用智能计算机模型应对不断变化的欺诈策略

人工智能 (AI) 能够让设备具备一定的推理和学习能力。机器学习是人工智能的一种高级形式，它让计算机模型无需精密编程便能够具备学习能力。

由于智能计算机模型能够通过各种反馈机制不断学习，因此可以提供越来越准确的结果并产生新的洞见。

为了充分发挥自动欺诈筛查解决方案的作用，应为计算机模型提供大量的优质交易数据供其提取。欺诈筛查解决方案还应提供更高级别的精确控制，有效整合计算机分析和相关规则，将人类智慧和业务相关参数融入其中。

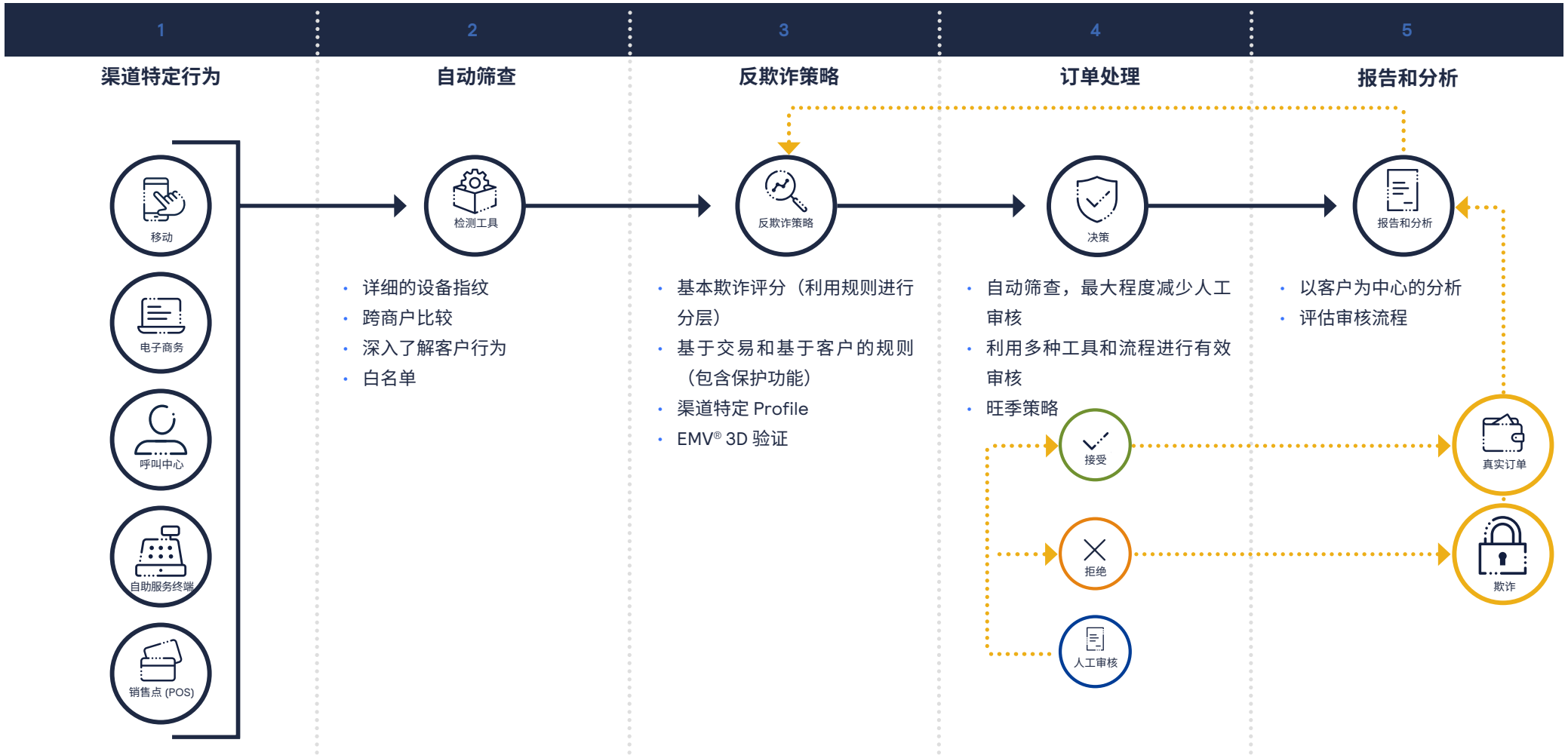
在欺诈者不断变换策略的同时，智能计算机模型也能够不断学习、调整和挖掘新兴模式，从而帮助您有效防范欺诈。

明确人工欺诈筛查的作用

在开展电子商务的初期，对一开始收到的少量订单进行人工检查或许具有一定的可行性。但是，随着订单数量的增加，人工欺诈筛查可能会变得既费时又昂贵。如果人工审核员无法跟上进度，导致订单处理搁置，可能还会对客户体验造成负面影响。当电子商务业务进入这一阶段，就需要考虑实施反欺诈管理系统，采用自动化的处理方式了。

对于在自动筛查时难以判定为接受或是拒绝的交易，则应对其进行人工审核。此时，审核员可以应用更多技术，并利用自身对于业务以及客户的了解来确定订单是否真实。还可将人工审核结果作为一种反馈资源，借此来不断优化筛查解决方案中的规则和计算机模型。CyberSource 机器学习模型与灵活规则引擎的强大组合，能够迅速、准确地响应独特或新兴的欺诈趋势。

根据特定的业务需求打造适合自己的反欺诈管理模式



应将哪些工具纳入反欺诈管理策略？

将带有 EMV® 3D 验证和欺诈预测分析的筛查工具加入您的候选名单

为贵组织的反欺诈管理策略考虑一种最佳的解决方案和服务组合。

反欺诈筛查工具：

验证服务

- 邮寄地址验证服务
- 电话号码验证
- 电子邮件验证
- 地理指标和地图
- 生物识别指标
- 卡验证值 (CVV) 验证
- 地址验证服务 (AVS) 验证
- 双因素电话验证
- EMV® 3D 验证
- 信用历史认证
- 支付公开记录服务

您的专有数据和客户历史记录

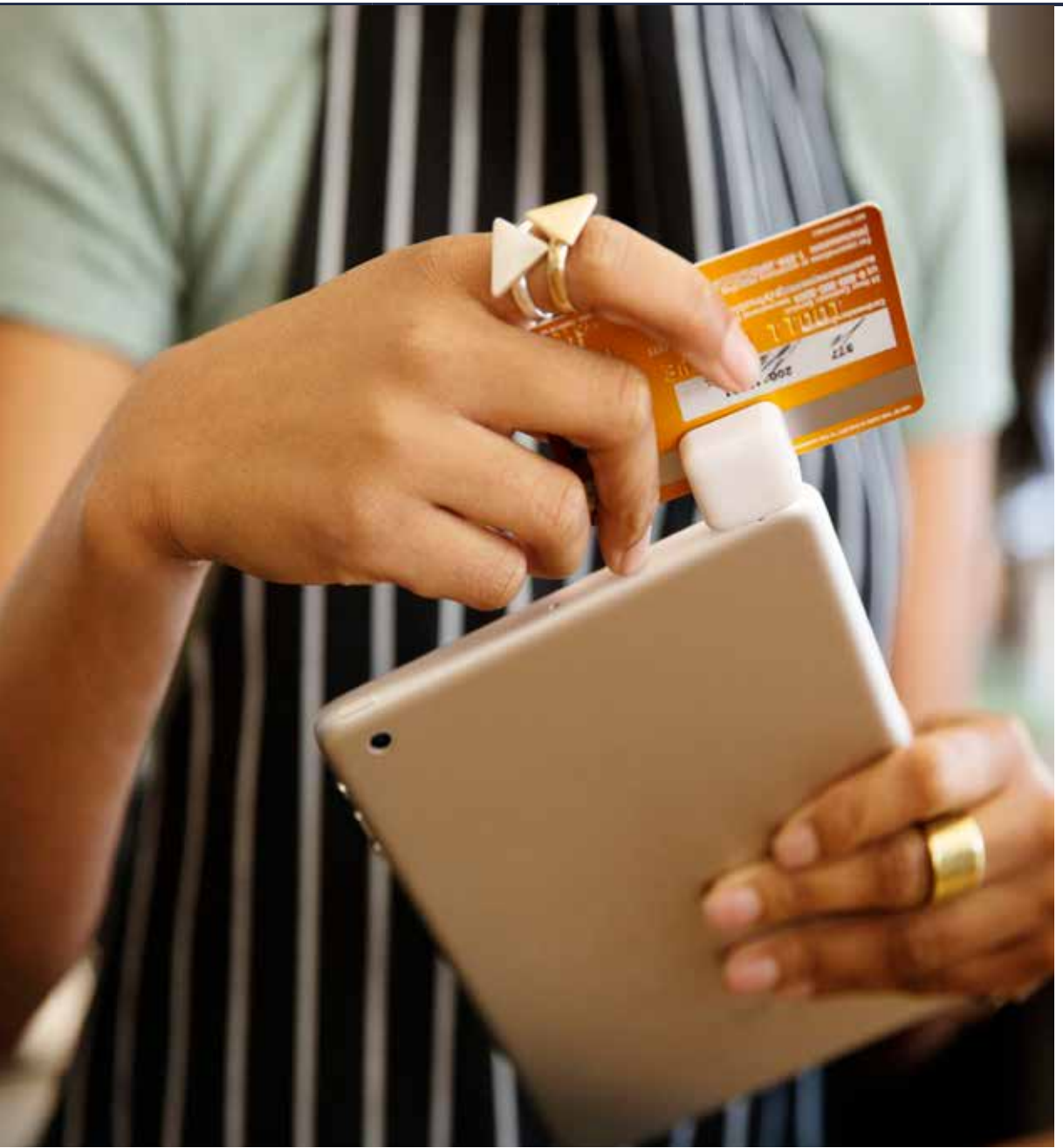
- 欺诈评分模型（公司特定）
- 客户网站行为和模式分析
- 客户订单历史记录
- 黑名单（内部名单）
- 白名单（内部名单）
- 订单频率监控
- 代理检测

多商户数据和购买历史记录

- 第三方聚合商提供的信用卡欺诈警报服务
- 共享黑名单（也称为红名单）
- 多商户购买频率和身份变化模型

购买设备跟踪

- 地理定位 - 笔记本电脑、台式机、移动设备和平板电脑
- 设备指纹识别
- Web 浏览器 IP 地址



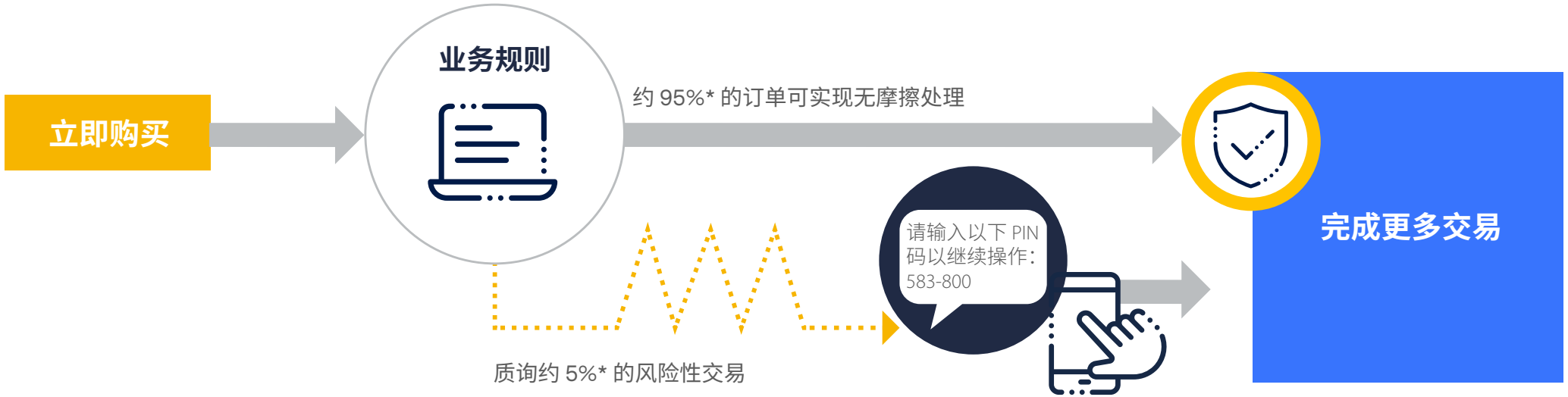
防范欺诈性拒付

EMV® 3D 验证能够帮助您阻止与欺诈有关的拒付。这项技术让您能够实时验证在线交易中的付款人身份。

为避免在结账过程中引入不必要的摩擦，应采用基于规则的方法，让您能够决定何时需要请求进一步的验证。您可以通过 3D 验证仅针对最具风险的交易发送验证请求，这让您既能够保证客户体验，降低结账放弃率，又能够继续从责任转移中受益。此方式仅适用于不受 SCA 指令约束的地区。

在对交易进行 3D 验证时，银行卡方案可能会对发卡行施加相关法规，将欺诈性交易的金融责任转移给发卡行。这就是所谓的责任转移，商户应务必了解其所在地银行卡方案中的相关法规，这是涉及其自身利益的重要信息。

利用 Cybersource 基于规则的 3D 验证始终如一地提供无摩擦的客户体验



订单结算

- 仅使用预配置验证规则质询所选订单

基于风险划分订单处理流程

- 智能规则引导高风险客户接受质询

业务成果

- 减少因交易摩擦而造成销售损失的风险
- 减少拒付
- 潜在手续费节省
- 责任转移
- 减少人工审核

*仅为说明性示例。
适用于不受 PSD2 SCA 或任何其他客户验证指令约束的市场。

最佳反欺诈管理中有哪些诀窍？

利用 Cybersource 欺诈预测技术

全面的多层次反欺诈管理策略，利用先进的机器学习和人工智能，可实现有效防范欺诈、无缝客户体验和高效运营之间的最佳平衡。我们的专家可以在 Cybersource 反欺诈管理解决方案的实施过程中提供协助，从而帮助您提高决策准确性、实现增收并从深厚的专业知识中受益。

提高准确性

Cybersource 利用独一无二的机器模型生成风险评分，该模型由拥有数十年经验的 Visa 和 Cybersource 数据科学家构建和维护。这些模型从全球数十亿笔交易中获取洞见，每笔交易的数据字段可达数百个之多，其中包含设备指纹、IP 地址、地理定位等信息。凭借如此大量且实时更新的丰富数据，Cybersource 无与伦比的机器学习模型能够帮助企业更快更准确地检测出新型欺诈模式并减少误报。

实现增收

优化授权以实现增收是平衡化反欺诈管理策略中的下一个关键步骤。发卡行的电子商务授权率仍远远落后于实体授权率。Cybersource 正在努力通过调整交易处理方式来缩小两种方式之间的授权率差距。我们的“营收获取”计划致力于为发卡行提供更大的可见性，使其在做出授权决策时能够掌握更多信息，借此来改变企业与发卡行之间的交互方式。

请阅读我们的“营收获取”白皮书以了解更多信息。

企业级欺诈预测技术可分析每笔交易的风险概率。Cybersource 提供独一无二的反欺诈管理解决方案，内含多种机器学习模型，基于 Visa 和 Cybersource 数十年的全球经验积累。

Cybersource 反欺诈管理解决方案基于深厚的反欺诈领域专业知识

超过 20 年

的**机器学习模型**和基于规则的反欺诈管理软件开发经验

超过 800 年[13]

的综合性**专业知识（覆盖数十个垂直领域和地区）**，由超过 65 位分析师面向五大洲提供咨询服务

24/7

全天候可享的附加服务，包括欺诈筛查员服务，可协助您**管理旺季业务**或处理大量人工审核

数万亿[13]

美元的**在反欺诈管理软件**、硬件和人员上的持续资金投入

[13] 截至 2020 年 8 月 1 日

Cybersource 推出了一系列面向大小各类公司的反欺诈管理解决方案

先进的全套反欺诈解决方案和服务，可满足您的各类需求

中小型业务

基础版反欺诈管理

基础版反欺诈管理是独一无二的支付网关反欺诈管理解决方案，采用企业级 Cybersource 欺诈预测技术，并内置简单的预配置欺诈设置。具有风险交易自动检查功能，并允许用户根据业务方式设置交易筛选条件。

- 通过可靠的筛查和强大的基于机器学习的计算机建模来检测欺诈。
- 利用内置反欺诈规则和预配置设置缩短设置时间。
- 降低拒付率，减少由卡测试和常见欺诈攻击导致的授权成本。
- 用户可利用简单直观的面板做出明智的决策。
- 欺诈保护功能不会对客户造成任何不利影响，能够在不增加结账摩擦的情况下有效降低欺诈率。

获取双重优势，随时可用的反欺诈解决方案，以及可访问的欺诈检测技术。

账户冒用保护

根据您的规则积极监控新账户创建和账户使用情况，保护客户账户，防止欺诈者非法使用相关支付数据。

企业级业务

Decision Manager

利用强大的检测测试、筛查模型、案例管理功能和实时报告简化反欺诈管理操作。Cybersource Decision Manager 兼有复杂的机器学习模型和灵活的规则引擎，能够迅速、准确地响应独特和新兴的欺诈趋势。

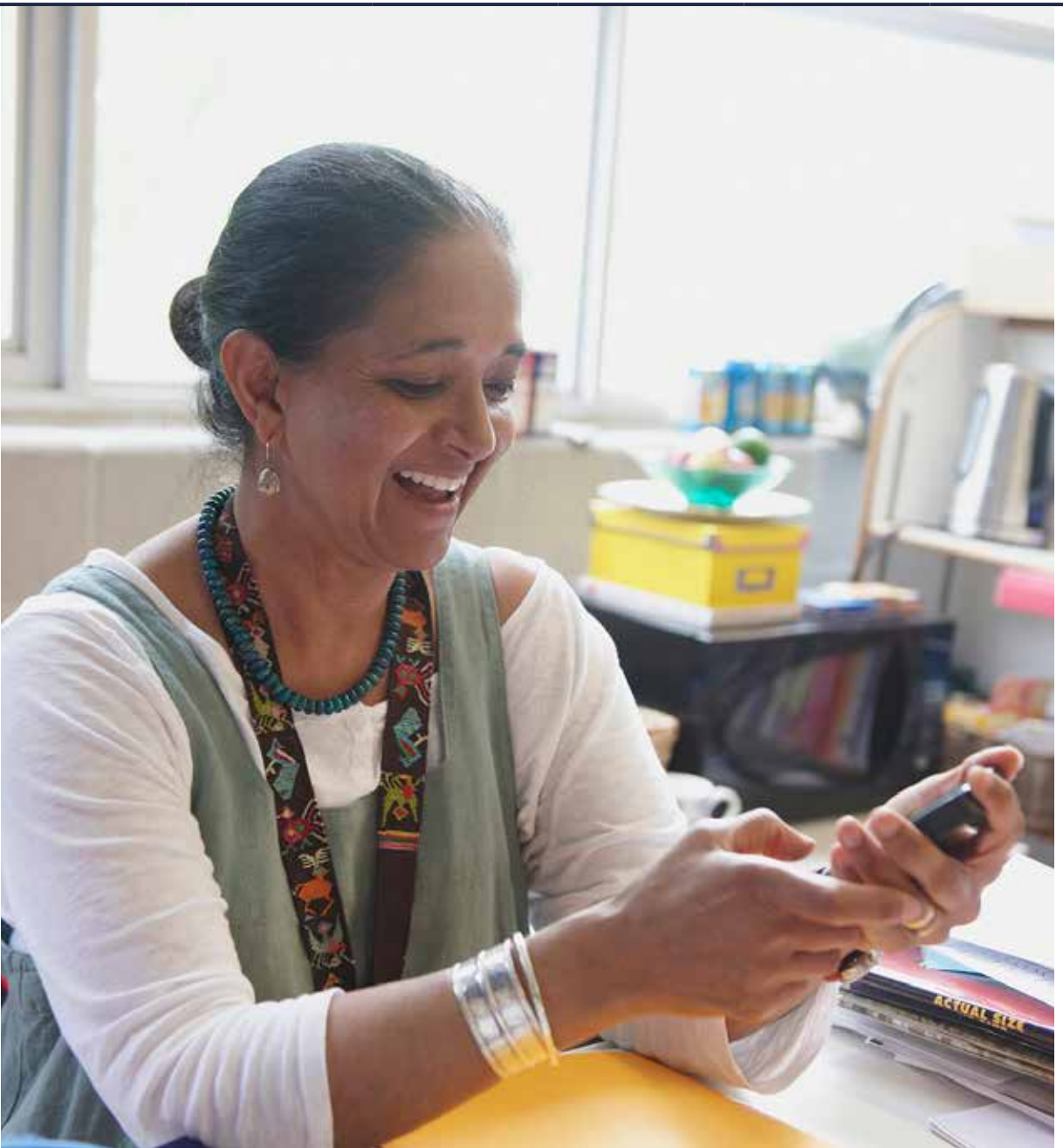
- **Rules Suggestion Engine：**将 Decision Manager 的高级机器学习应用于历史交易数据，自动生成新规则建议，无需任何人工干预。
- **Decision Manager Replay：**将测试时间从几个月缩短至几分钟。根据您的历史交易数据对不同的“假设分析”反欺诈策略进行测试，以评估反欺诈策略调整的影响。

托管式风险服务

聘用专家组成 Cybersource 风险分析师顾问团队，面向五大洲提供咨询服务，以优化 Decision Manager 的分析结果。24/7 全天候可享的筛查管理资源附加支持，可协助您进一步扩充运营能力。

账户冒用保护

根据您的规则积极监控新账户创建和账户使用情况，保护客户账户，防止欺诈者非法使用相关支付数据。



更多反欺诈和风险管理解决方案

交货地址验证

验证输入的地址信息，并更正 200 多个国家/地区订单中的无效城市、省/市/自治区、邮政编码组合。

欺诈警报

让您能够近乎实时地收到消费者已确认的欺诈通知，从而及时停止发货、节省执行成本并防止拒付。

忠诚度反欺诈管理

实施全面的反欺诈管理解决方案，通过数百次的欺诈检测测试分析访问行为、监控可疑账户更改并分析结账购买，同时提供 Cybersource 账户冒用保护。

EMV® 3D 验证

指明规则以确定对哪些交易执行 3D 验证，对哪些无需执行验证，以此来改善客户的结账体验。

术语表

了解电子商务反欺诈管理的基本概念和术语

账户冒用欺诈：利用盗取的登录凭证控制账户并实施欺诈。

地址验证服务 (AVS): 一种工具，用于验证客户在订购过程中提供的地址和邮政编码。验证时会将地址的数字部分与客户发卡行所记录的卡信息进行比较。

人工智能 (AI)：通常需凭借人类智慧才能实现的技术执行功能，例如推理和学习。

卡验证值 (CVV): 客户在购买过程中提供的支付卡上的三位数或四位数安全码。银行通过查看此代码来验证银行卡在购买时是否被出示。

拒付：当客户就其银行卡对账单上的商品提出争议并被成功受理后，发卡行撤回对企业账户付款的过程。

“毫无破绽”的欺诈：一种欺诈形式，利用盗取的信用卡和持卡人信息实现线购买行为表面上的合法化。

电子商务：利用网络、移动或其他技术在线购买或出售产品。

EMV（Europay、Mastercard 和 Visa）技术：将计算机芯片嵌入信用卡中，以实现持卡人数据的安全存储，有助于防范实体店欺诈性购买。（也称为“Chip-and-Pin”（芯片密码）技术。）

无限货架：一种购物体验，让店内客户能够在线轻松浏览和订购多种处于缺货状态或者店内并不销售的产品，并将其运送到商店、家中或其他地点。

第一人称欺诈：一种欺诈形式，持卡人声称购买未经授权或商品未送达，以此来索要赔偿。客户获得赔偿，但却可以将商品归为己有。（也称为友好欺诈）。

欺诈筛查：一种预测性分析方法，利用当前和历史数据来评估风险。

灰色市场欺诈：利用盗取的信用卡购买商品，然后将这些商品销售到未经授权的市场或地区，或将其打折出售。（也称为经销商欺诈。）

责任转移：如果交易经 EMV®3D 验证核实后发现存在欺诈性验证，发卡行将需要承担财务责任（循环交易除外）。

机器学习：人工智能的一种高级形式，它让计算机模型无需精密编程便能够具备学习能力。

人工审核：对于自动筛查过程中难以判定为接受或拒绝的订单所采用的一种由人员亲自进行审核的流程。

黑名单：一类列表或数据库，内容包含：信用卡详细信息、客户名称、电子邮件地址、实际地址，有时还包含被识别为欺诈或有风险的整个国家或地区。（也称为红单表。）

全渠道：一种业务策略，致力于跨电子商务和传统销售渠道提供无缝的客户体验。

3DS 验证：一项技术，让您能够实时验证在线交易中的付款人身份。（也称为 EMV® 3D 验证。）

支付服务指令 2 (PSD2)：PSD2 是由欧盟国家设计的第二套支付服务指令。于 2018 年 1 月 13 日实施。可能会对支付行业的方方面面产生重大影响，包括在线支付方式，以及支付时将会看到的信息内容。

词汇表（续）

白名单：一类列表或数据库，包含已知的无风险和低风险客户或银行卡，与其相关的订单可直接批准，无需进行审核。

退款或退货欺诈：利用盗取的凭证在线购买商品，然后前往实体店领取退款或礼品卡的过程。

重新运送欺诈：一种欺诈行为，利用盗取的支付详细信息购买商品，然后联系托运公司，要求将商品运送到新地址，或者付钱给一些人（即所谓的货运代理人）来接收商品并将其重新运送至其他地点进行转售。

规则系统：一种解决方案，利用 if-then 逻辑方法来触发不同的反欺诈管理功能。

统计评分模型：一种基于已知的客户资料信息（例如订单历史记录、购买频率、设备跟踪和先前的欺诈记录）的交易评估方式。

强客户身份验证 (SCA)：欧洲银行业管理局在支付服务指令 2 (PSD2) 中新增的针对身份验证的监管技术标准。根据 SCA 的规定，消费者需要通过以下三种方式中的两种来验证其身份：展示自己的身体特征（使用生物识别）；他们所独有的东西（信用卡、移动设备或令牌生成器）；以及他们所知道的信息（PIN 或密码）。

可疑活动监控：一种解决方案，用于检测可能属于账户冒用的欺诈性活动

第三方欺诈：一种欺诈行为，方式为利用持卡人的信息进行未经授权的购买。

EMV® 3D 验证：一项技术，让您能够实时验证在线交易中的付款人身份。（也称为 3DS 验证。）

了解更多

了解 Cybersource 能够通过哪些方式来帮助您防范欺诈、简化客户体验并控制成本

电子商务欺诈将会愈演愈烈。通过采用全面、多层次的反欺诈管理方法，贵组织可以最大程度地防范欺诈并提高运营效率。同时打造卓越的客户体验，并实现电子商务业务的增收。

深度挖掘

探索各类 Cybersource 反欺诈管理解决方案：**www.cybersource.com/fraud**。纵览全球各大电子商务领导者的最佳实践，掌握成为“平衡掌控大师”的秘诀。并免费下载我们的全球反欺诈报告：**www.cybersource.com/fraudreport**。

联系我们

欲知更多信息，欢迎访问：**www.cybersource.com**

cybersource
A Visa Solution