Cybersource+ 专家：
2022 年欺诈趋势报告

反欺诈前景展望

在瞬息万变的世界中确保增长

cybersource
A Visa Solution

目录

身处瞬息万变的世界，万事皆应准备周全

过去几年与以往不同，世界各地的企业迅速抓住了由电子商务激增、不断变化的消费者和欺诈行为及政府和监管需求带来的新机遇，表现出非比寻常的弹性。

现在是时候为下一步做好准备了。

我们邀请来自商家风险理事会 (MRC)、Aite-Novarica 和 CyberSource 的专家团队，分享其对未来欺诈的真知灼见，并帮您制定减少欺诈且能够带来更多业务的策略。

深入了解：

1. 疫情如何改变欺诈行为
2. 自动化欺诈者崛起
3. 需要警惕的欺诈趋势
4. 四步启动反欺诈策略

我们的专家团队

Tracy Kobeda Brown

商家风险理事会 (MRC) 项目与技术副总裁

Tracy 是一位经验丰富的高管，从初创企业到财富 500 强公司，都留下了她的身影。她的技能涵盖技术战略、产品设计、用户互动、游戏、移动和信息安全领域。

在业余时间，她会玩电子游戏，并自愿担任初创企业的教练和行政顾问。在见过著名主持人奥普拉后，她的愿望是开设一个动物收养所，写一本书，并为执法部门建立新的技术解决方案

David Mattei

Aite-Novarica Group 战略顾问

David 在支付行业设计、构建、启动欺诈和争议系统方面拥有超过 15 年的经验。他的客户包括商户和金融机构，这使他能够以独特而全面的视角看待问题。

David 的梦想是买一张去欧洲的单程票，游览完所有想去的景点后再回家。他还想买下他祖母出生的意大利村舍。

Mari-anne Bayliss

Cybersource 欧洲区域解决方案高级总监

Mari-anne 与欧洲商户合作，了解各地的欺诈趋势，确保在产品开发中反映出这些趋势的特点。她曾为英国一家大型零售商工作，拥有 20 年的反欺诈经验。

工作之余，Mari-anne 通过为家人和朋友展示厨艺来放松自己。她是一位激情四射的糕点师，梦想是参加“英国烘焙大赛”(Great British Bake Off)。

Martin Lee

Cybersource 亚太区风险管理服务部门总监

Martin 拥有超过 15 年的反欺诈经验，领导着一支由来自整个亚太地区的专家组成的团队。他们的职责是代表使用 CyberSource 风险解决方案的客户管理反欺诈策略。

Martin 来自英国，现居新加坡，他是一个超级足球迷，大多数的周末都在深夜观看比赛。

Mark Strachan

Cybersource 全球服务总监

Mark 是一名欺诈风险专家，在支付和银行业拥有超过 12 年的经验。他与零售、数字和票务等行业的商户合作，制定降低欺诈活动相关风险的策略。

闲暇之余，Mark 喜欢探索新的旅行目的地、爬山、在家做饭，或者沉迷于他热爱的戏剧。

1 疫情改变了欺诈行为

“电子商务销售额的增长令人惊叹。回顾 2021 年，全球的电子商务销售额呈现出显著增长。如果没有疫情因素的影响，全球电子商务销售额可能需要数年时间才能达到我们现在的水平。”

David Mattei
Aite-Novarica 战略顾问

疫情相关限制促使线上销售额飙升。然而，这不可避免地导致全球范围内针对商户的欺诈攻击有所增加。最近的研究表明，约四分之三的商户表示，与疫情前相比，欺诈企图和欺诈率都有所增加。[1]

因此，有十分之九的商户认为管理电商欺诈对于其整体业务战略“非常重要”或“极其重要”[2] 也就不足为奇了。

消费者心态发生变化

刚接触电子商务的消费者可能没有意识到潜在的风险，或者没有做好应对的准备。随着向数字化的转变，欺诈者找到了新的犯罪方式。

社交媒体对许多人而言成为新的游乐场 - 在短短 12 个月内，就有超过 5 亿用户加入了社交媒体平台。[3] 尽管在教育人们认识在线欺诈和诈骗的风险方面付出了相当大的努力，但在社交渠道上很容易就会过度分享个人详细资料，这使欺诈行为接踵而至。

如需关于欺诈者如何利用社交媒体进行身份盗窃的更多信息，请参阅第 2 章。

还有一个重要的发展趋势：消费者导向欺诈，即伪善（或第一人称）欺诈的增加。商户将伪善欺诈列为 2021 年遭遇的最常见的欺诈攻击类型，高于 2019 的第五位[4]，并估计他们接受的电子商务订单中约有 1.2% 最终被证明属于伪善欺诈。[5]

在第 3 章，我们将讨论伪善欺诈和一种类型相似的欺诈，即政策滥用。

1 《2021 年全球反欺诈报告》，Cybersource 和 MRC，2021 年，第 7 页
2 《2021 年全球反欺诈报告》，Cybersource 和 MRC，2021 年，第 6 页
3 “去年有 50 亿用户加入了社交网络（以及其他数据）”，hoosuite.com，2021 年 7 月
4 《2021 年全球反欺诈报告》，Cybersource 和 MRC，2021 年，第 17 页
5 《2021 年全球反欺诈报告》，Cybersource 和 MRC，2021 年，第 17 页

商户作出调适

疫情期间，由于团队成员居家办公或被暂时解雇，许多反欺诈团队都面临着重重压力。与此同时，随着订单量的增加，反欺诈团队的资源往往捉襟见肘。

对于一些商户来说，这种体验就像是延长的销售旺季。在这段如此长的旺季里，他们很难为反欺诈团队补充人手。为了追求客户体验，一些在过去会被拒绝的订单现在可能会被放行。这意味着，即使收入增加，欺诈率也可能会增加。

无摩擦流程

在这场疫情中，流畅的体验变得越来越重要。对于在线购买、到店取货 (BOPIS) 和路边取货购买来说尤其如此，因为选择此类购买方式的客户希望快速完成订单。他们可以在一两个小时内取货，因此在决定接受还是拒绝此类订单之前就没有时间进行审查 - 这可能会增加企业的欺诈风险。

“疫情颠覆了商户对欺诈的传统认知。例如，伪善欺诈与商户先前遭受的攻击属于不同的数量级，因此他们不得不改变筛选和审查方式。”

Tracy Kobeda Brown
MRC 项目与技术副总裁

疫情前，我们看到商店在客户取货时将自动审查与物理安全措施相结合，如检查身份证件和匹配支付卡。

现在，我们看到商户在订单进入取货阶段之前，使用欺诈筛查功能来辨别异常情况 - 包括结合机器学习来进行自动检测、建立全球黑名单，以及使用更先进的多变量频率，如多个取货地点与单一身份相关联。

这种情况下，一种反欺诈管理分层方法应运而生，我们将在第 4 章探讨这一主题。

“一些零售商所经历的收入斗争导致了反欺诈经理（他们认为自己的角色是防范诈骗）和负责增收的人员之间的‘拉锯战’。您愿意承担多大的风险来换取更多的收入呢？”

Mari-anne Bayliss
Cybersource 欧洲区域解决方案高级总监

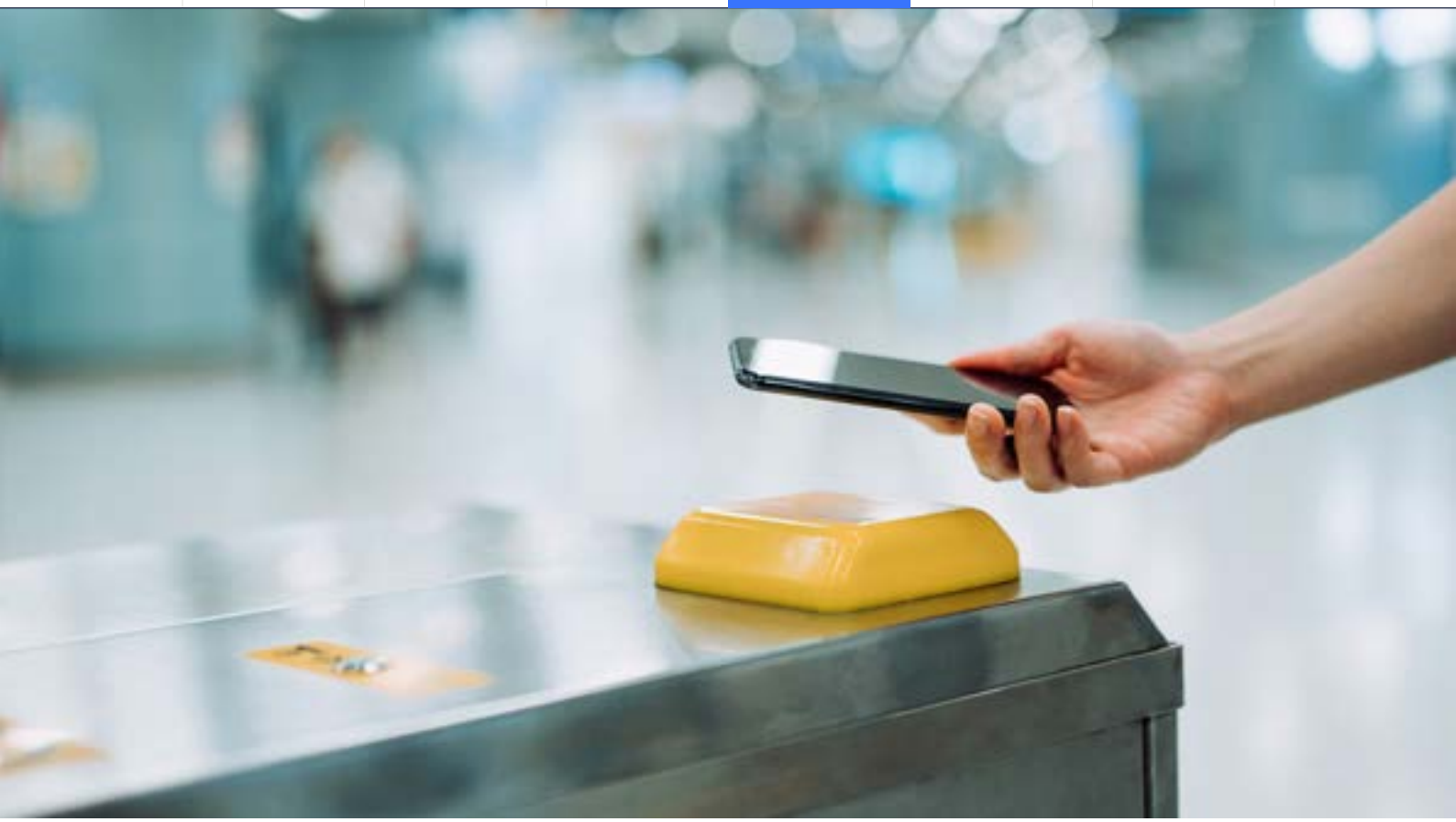
欺诈者紧跟时代步伐

甚至早在疫情爆发之前，一种新型欺诈者就已经出现：他们更有组织性、更自动化，通常作为团体或团伙的一部分出现，而不是单独行动。

- **重点已从支付环节的欺诈转移到对整个身份的窃取。**随着越来越多的消费者进入数字化时代，欺诈者迅速利用漏洞窃取数据，使用真实、虚假或合成的身份建立全新账户。
- **欺诈者迅速利用不断发展演变的订单履行方式规避反欺诈工具。**以 BOPIS 为例，并没有在其中捕获到送货地址，或类似伪善欺诈的欺诈性转售活动。

关键信息

将风险管理延伸到支付之外，将整个端到端流程纳入考虑 - 包括从创建账户到发货或收货，甚至到退货流程。确认存在风险的环节，填补漏洞，维持最佳客户体验。



2 自动化欺诈者崛起

身份盗用和数据泄露已成为网络犯罪的两大驱动因素，特别是在欺诈者意识到窃取身份远比单纯欺诈攻击更有价值的情况下。欺诈者的传统作案手法已经不再奏效：过去，他们通常可以将窃取的支付详情使用数周时间，但现在他们不敢再有这种奢望。网上和手机银行应用中的账户每天会被检查数次，所以窃取的详细信息可能只在几小时内有效。

如今，欺诈者通过窃取身份数据建立“干净”账户，这些账户在数周内一直都是可用的。我们发现：

- **巧妙识别身份盗用**和创建虚假账户。
- **自动化程度提高：**欺诈者一旦发现新漏洞，就会采用最新的技术（机器人、聊天机器人和验证码绕过技术，甚至人工刷单）立即发起攻击。[6]
- **显而易见的欺诈：**其他欺诈者逐渐将暗网抛在脑后，直接将技术和策略运用到社交媒体上。

6 “网络安全警告：黑客利用自动化技术加强攻击的 10 种方式”，ZDNet，2020 年 3 月

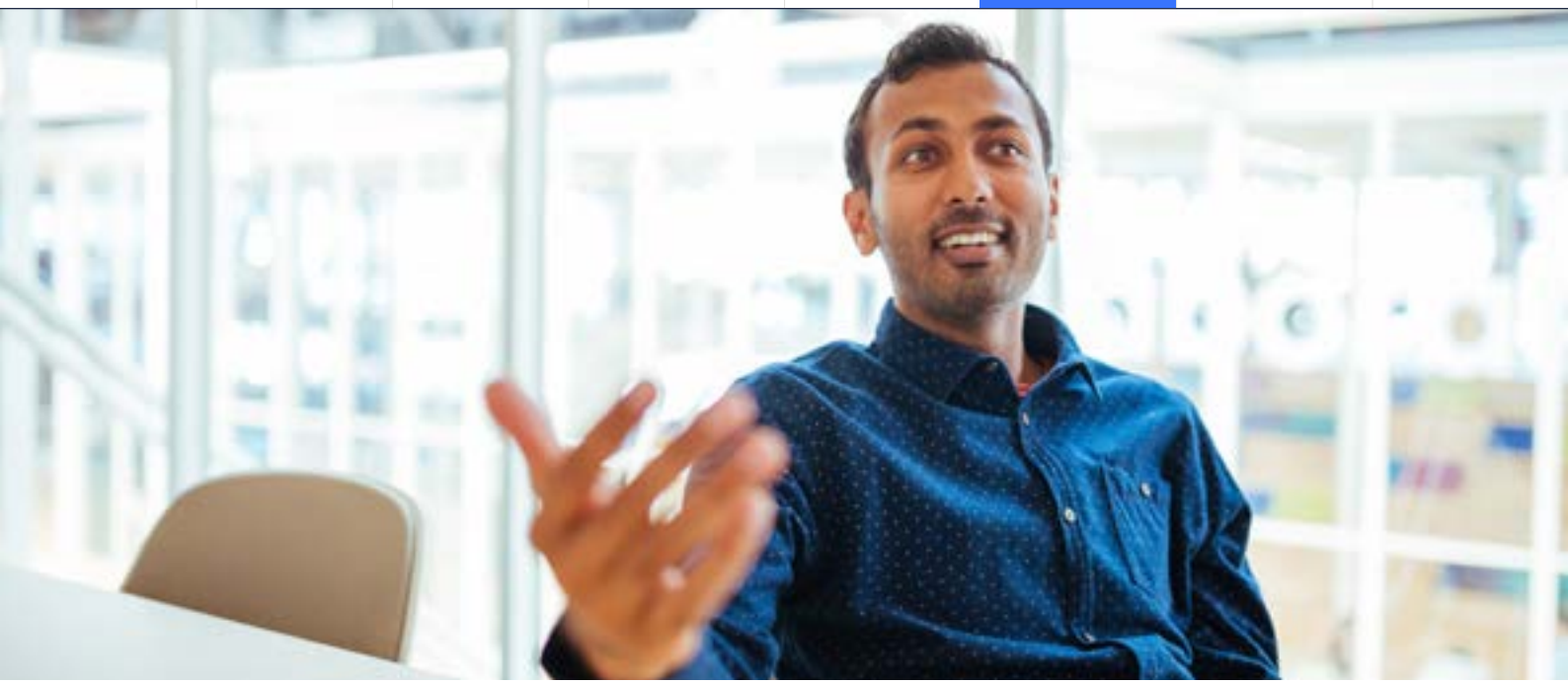
聚焦：
利用社交媒体窃取身份

欺诈者试图通过多种途径窃取身份数据，从非法侵入、社交工程到大规模数据泄露，不一而足。自疫情爆发以来，随着一大批新用户的加入，社交媒体为新型诈骗提供了肥沃的土壤。

我们发现社交媒体用户：

- **在他们的账户上发布**诸如全名、出生日期以及居住地或工作地点照片之类的信息
- **使欺诈者很容易**就能通过梳理朋友和家人的信息搜集到他们母亲的婚前姓氏
- **回答看似无害的弹出式测验问题**。例如，通过询问您出生时哪首歌曲排名第一，欺诈者会发现您的出生年份和月份。通过将其与您的出生日期（社交档案中通常会包含该信息）相结合，这种精心设计的网络钓鱼行为就会使您的完整出生日期泄露
- **回应欺诈者冒充新联系人**提出的个人问题，例如，最喜欢的运动或第一只宠物的名字（通常用作忘记密码时的提示）

欺诈者可以毫不费力地获得上述所有信息，从而能够访问客户的在线账户，或建立完整的客户身份，在其他网站上进行欺诈。



3 注意事项

在接下来的一年里，有许多领域的欺诈者可能会特别活跃，对此应保持警惕。

账户冒用和忠诚度欺诈引发担忧

新账户发起欺诈、利用合成身份的新账户欺诈和账户冒用欺诈（当欺诈者非法访问或操纵客户账户数据时）仍然都很严重。数据泄露可能导致数百万条包含个人身份信息 (PII) 数据的记录被泄露，是欺诈者进行数字账户攻击的猎物。

防止账户冒用应成为监控工作的关键部分，以帮助您了解：

- 谁在为您创建新的在线账户
- 谁在登录现有账户
- 谁试图更改关键账户信息，如密码或配送地址

数据泄露和其他形式的身份盗用，意味着欺诈者可以拥有正确的用户名和密码来访问现有账户，或拥有令人信服的数据组合来建立新账户。确保您的反欺诈解决方案会对账户活动进行检查，以确定真实账户访问或创建的可能性。

“我们最近看到的一些攻击手段是在旧手段的基础上做出的改变。例如，新账户欺诈，即创建合成身份，建立与任何人无关的虚假账户，而这些账户正在被美化，准备在未来进行使用。”

David Mattei
Aite-Novarica 战略顾问

忠诚度奖励计划欺诈正愈演愈烈，在旅游和酒店业尤为严重。对于我们大多数人来说，最近旅行的机会是十分有限的。如果我们不旅行，我们就不会像以前那样经常查看航空公司和酒店的奖励计划，这使欺诈者有机可乘。当欺诈者侵入这些账户后，他们可以迅速将积分转化为金钱。

那些能够保护您的企业和客户免受欺诈性账户创建和接管的工具，应该也能够防止忠诚度计划滥用。

“直到最近，旅行限制意味着窃取和兑换积分对于欺诈者来说没什么好处。然而，随着旅行的放开，他们已为利用这一优势做好了准备。除了使用技术来防止账户接管外，让客户了解监控账户的重要性也是至关重要的。”

Mark Strachan
Cybersource 全球服务总监

三种用于支付欺诈的数据盗窃

我们建议优先解决这些形式的数据盗窃问题。它们都可以用于在线卡测试和凭证填充，这些是目前许多账户接管攻击的特征。

1

利用恶意访问窃取数据

长期以来，欺诈者一直使用暴力破解攻击、网络钓鱼、短信欺诈和恶意软件等手段恶意访问数据。

除此类攻击的增加外，[7]我们还发现欺诈者利用居家办公人数的增加来获利。欺诈者试图通过伪造经理和董事的电子邮件地址来冒充他们，说服员工提供访问网络资源的凭证，从而窃取数据。

2

休眠账户：放长线钓大鱼

发生在 2020 年初的数据泄露事件，使欺诈者能够在疫情开始之际建立新的在线账户。这些账户隐藏在真实客户第一次在线购物时创建的大量新账户中。

许多情况下，欺诈者直到很久以后才会使用这些账户，因为他们认为通过旧账户进行的交易不太可能受到欺诈筛查。先进的反欺诈工具可以识别并封锁这些账户。

3

随着强客户认证的启动，SIM 卡调换呈增加趋势

SIM 卡调换，又称为 SIM 卡劫持或 SIM 卡窃取，允许欺诈者控制个人手机账户。诈骗者利用从社交媒体收集的信息或在数据泄露中窃取的信息，冒充账户所有者，说服手机公司将账户从所有者的 SIM 卡转移到欺诈者控制的 SIM 卡上。

随后，欺诈者就可以拦截包含一次性密码 (OTP) 或个人识别码 (PIN) 的短信，这些代码用于在线购买时的强客户认证 (SCA)。PSD2 SCA 在欧洲的推出意味着对 OTP 和 PIN 更加依赖，SIM 卡调换攻击可能会愈演愈烈。

7 “国际刑警组织报告显示，新冠肺炎期间网络攻击增长速度惊人”，国际刑警组织 (INTERPOL)，2020 年 4 月

聚焦：
伪善欺诈和政策滥用增加

伪善欺诈（又称第一方欺诈）的发生场景如下：客户用支付卡在线购买产品或服务，然后联系发卡方，就费用提出异议，例如，声称没有收到商品或收到损坏的商品。

当客户试图操作商户退货和退款流程时，或者退款所需时间太长时，这种情况也会发生。

“要处理和阻止伪善欺诈，商户需要进行大量的运营工作。这会影响收入损失和预测，因此商户不会积极处理这一问题。事实上，伪善欺诈并不是友好的。”

Martin Lee
Cybersource 亚太区风险管理服务总监

我们的专家指出，在过去，伪善欺诈通常与人们投机取巧的行为有关 - 可能是利用商户流程中的漏洞。

如果商户发现了伪善欺诈案件，并就此质询客户，他们通常就会收手。但伪善欺诈行为正在不断增长和演变，这也许是因为疫情带来的经济效应使消费者更具创新精神，而且谎称没有收到包裹也不会受到太多的惩罚。全球的商户都表示，目前伪善欺诈是他们遇到的最常见的欺诈攻击，卡测试、网络钓鱼和身份盗窃紧随其后。

企业遇到过的前 5 大欺诈（按企业规模划分）

小微企业

1. 伪善欺诈
2. 卡测试
3. 钓鱼攻击/网域嫁接/鲸钓攻击
4. 身份盗用
5. 优惠券/折扣/退款滥用

中型企业

1. 伪善欺诈
2. 卡测试
3. 身份盗用
4. 钓鱼攻击/网域嫁接/鲸钓攻击
5. 优惠券/折扣/退款滥用

大型企业

1. 伪善欺诈
2. 卡测试
3. 钓鱼攻击/网域嫁接/鲸钓攻击
4. 忠诚度奖励计划欺诈
5. 优惠券/折扣/退款滥用

信息来源：《2021 年全球反欺诈调查结果》，Cybersource 和 MRC，2021 年

下面是我们从伪善欺诈中观测到的一些关键变化：

- **家庭欺诈**是伪善欺诈的一种形式，它源于家庭成员之间的设备共享，即任何家庭成员无需持卡人的许可就能进行应用内购买。持卡人可以通过提出异议/撤单的方式收回资金。
- **与数字商品相关的伪善欺诈**很难被证明，因为没有签名或其他交付证明。商户需要收集额外资料，以帮助其向银行证明客户确实下了订单。设备指纹识别、地理定位数据和行为生物识别技术都是很有用的工具。
- **伪善欺诈与欺诈性转售的关系可能越来越密切。**如果某个有组织的欺诈团伙实施了大量的伪善欺诈，最终可能会在线上转售赃物。
- 随着各国重新开放，消费者展现出超乎寻常的消费热情。这种消费冲动被称为报复性消费。[8] 这样**购买者更容易后悔**，从而使客户更有可能对交易提出异议。

8 “报复性经济的兴起”，Internet of Business，2021 年 8 月

伪善欺诈和政策滥用（全球第五大最常见的欺诈攻击类型[9]，包括优惠券、折扣和退款滥用）之间存在密切联系。

政策欺诈包括：

- **客户退回的商品与他们所购买的并不相同**。这可能相当明目张胆，例如，客户用假冒的名牌手提包冒充正品退回。
- **客户退回以 BOPIS 方式购买的商品**，却要求将款项退回到另外一张卡上。
- **职业退货师**在社交媒体网站上公开宣传他们提供的服务。他们将自己定位为退货政策方面的专家，能够制定策略以确保成功退款。在退款成功后，专业退款者会收取服务费，可能是商品价值的 20%。

为应对在过去两年中愈演愈烈的伪善欺诈，**全球 80% 的商户都采用正规方法对其进行打击**。[10] 大多数商户都选择了多管齐下的策略，包括发送客户通知，制定明确的支付和退货政策，以及实施用于检查和确认客户身份的各种验证措施。

伪善欺诈的增加正在挑战黑名单的神圣性，这意味着需要定期对其进行重新审视和清理。**考虑使用额外的筛选技术**（如 Cybersource Decision Manager 的 Identity Behavior Analysis，它广泛利用全球黑名单进行分析）来帮助做出接受/拒绝的正确决定。

“对于数字商品商户（如在线游戏）来说，伪善欺诈的确是一个严重的问题，他们向 Aite-Novarica 透露，高达 75%[11] 的退款都是由它造成的，这令人震惊。”

David Mattei
Aite-Novarica 战略顾问

9 《2021 年全球反欺诈报告》，Cybersource 和 MRC，2021 年，第 16 页
10 《2021 年全球反欺诈报告》，Cybersource 和 MRC，2021 年，第 18 页
11 “改善争议体验：透明度就是力量”，Aite-Novarica Group，2020 年 5 月

聚焦：
监管的影响越来越大

世界各地的商户一致表示，反欺诈管理挑战中最难的是适应法规或行业规则的不断变化，其次是应对新出现的欺诈攻击。[12]

PSD2 SCA 的出台就是一个很好的例子，它对向欧洲出口或在欧洲销售的企业产生了影响。尽管强客户身份验证 (SCA) 要求旨在通过双重身份验证来保护电子支付交易，但欺诈者仍试图找到规避法规的方法。SIM 卡劫持是欺诈者可能采取的众多途径之一，他们试图通过此方法获取用于 SCA 的 OTP 和 PIN，这种诈骗也呈上升趋势。

PSD2 SCA 推出后，越来越多的商户采用 EMV® 3-D Secure[13] (3DS) 来符合 SCA 要求。商户通过与反欺诈解决方案提供商合作密切，能够选择何时在客户支付体验中调用或禁止 EMV® 3DS，以及如何处理可能符合豁免条件或超出 SCA 范围的交易。

那些没有受到 PSD2 SCA 直接影响的企业正密切关注市场动向，以及 EMV® 3DS 在减轻电子商务支付欺诈方面发挥的作用，因为在一个地区行之有效的法规最终可能也会被其他地区采用。

12 《2021 年全球反欺诈报告》，Cybersource 和 MRC，2021 年，第 19 页
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。

4 制定能够获得更多业务的反欺诈策略

应对自动化欺诈者的方法有很多，制定与时俱进的反欺诈策略，以及进行循序渐进的改变，不仅对阻止欺诈者有所帮助，同时也有助于获得更多业务。

行动计划：四步启动反欺诈策略 〉

第 1 步：采取分层方法打击欺诈

任何一种单一的工具都无法满足您打击欺诈的所有需求。分层方法在整个客户体验中使用多种工具。确保您的反欺诈解决方案综合运用了以下工具：

账户级工具。**从账户创建起就开始进行欺诈筛查**。为识别和防止账户冒用，您需要对真实事件和高风险事件加以区分。包括账户创建、登录和更新，以及账户冒用欺诈。

CyberSource 的账户冒用保护 (Account Takeover Protection) 等解决方案包含设备指纹识别、行为生物识别和物理生物识别，以及一次性密码 (OTP) 等功能。

预筛查交易工具。在**与身份盗用、卡测试和凭证填充相关的订单导致授权被拒前就将其捕获**。预筛查工具可以在处理过程的上游使用，以便在授权之前检测欺诈行为。

为阻止欺诈，他们将机器学习与用户自己制定的策略相结合，在卡测试尝试以及授权费用产生之前进行拦截。

支付交易级工具。在 Aite-Novarica Group 最近调查的商户中，过半数[14] 仍依赖基于规则的方法管理在线支付欺诈。

为应对当今的自动化欺诈者，应使用先进的机器学习模型评估历史交易数据，并通过访问全球数据和行业洞察发现欺诈模式，为新的反欺诈策略提供信息。

工具配置的协调层。**使用机器学习自动进行风险校准**，以减轻反欺诈团队的负担并减少审查。先进的分析和报告有助于对这些工具进行优化，并且能够支持自行调节，因此您可以专注于业务而不是反欺诈。

“欺诈行为迅速发展的同时，传统的欺诈筛查规则却一直停滞不前，因此仅靠它们是完全不够的。您需要在规则、人工智能、机器学习和人工审查间找到一个合适的平衡点。”

Mari-anne Bayliss
Cybersource 欧洲区域解决方案高级总监

14 Aite-Novarica Group 在 2021 年对北美、欧洲和亚太地区 756 家中型和大型电子商务商户进行的定量调查

第 2 步：在反欺诈/摩擦中找到平衡

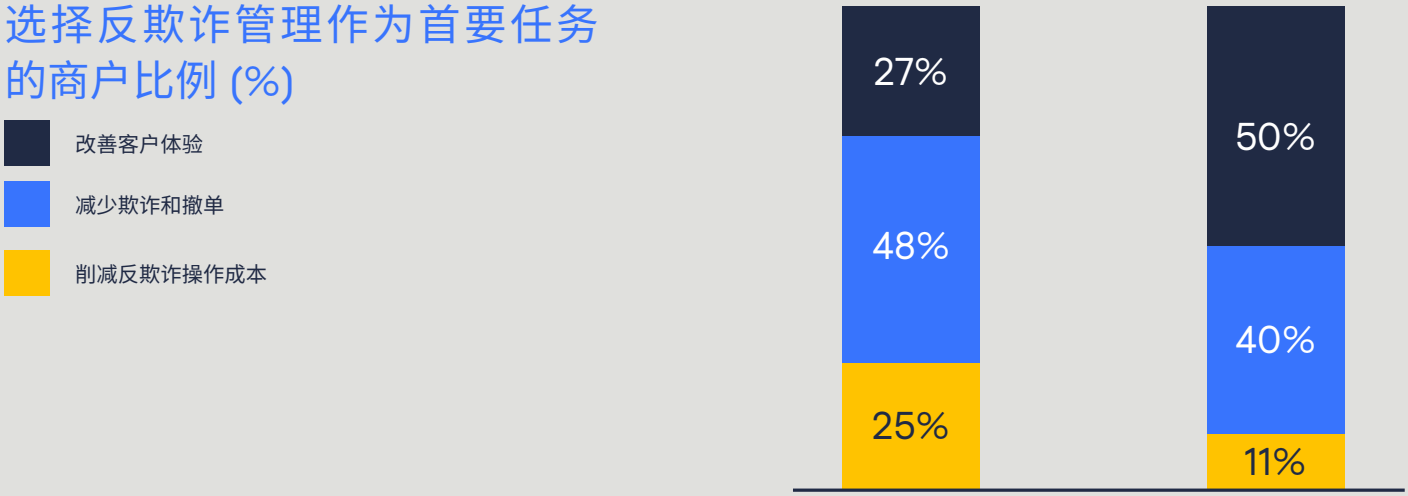
尽管攻击次数和收入损失都在增加，但有一半的商户表示，提升客户体验是他们在管理欺诈时的首要任务。[15]

仔细监控客户体验，让摩擦保持适中，避免过度增加。首先，应用在后台运行的低摩擦或无摩擦工具（如设备指纹和行为生物识别）。

当觉得可疑时，可以采用另一种识别方法，即使用机器学习和人工智能来识别交易另一端的人，或者让其参与一项任务，如输入 OTP。

这样您就可以最大限度提高批准率，最大限度减少欺诈损失，同时提供惊人的客户体验。

选择反欺诈管理作为首要任务的商户比例 (%)



信息来源：《2021 年全球反欺诈调查结果》，Cybersource 和 MRC，2021 年

“商户担心的是客户体验，因为摩擦和放弃购物都是他们不惜一切代价想要避免的情况。但是，除非将反欺诈组织加入对话，否则您真的无法谈论体验，因为反欺诈策略和部署的工具会对客户体验 (CX) 产生直接影响。”

Martin Lee
Cybersource 亚太区风险管理服务总监

15 《2021 年全球反欺诈报告》，Cybersource 和 MRC，2021 年，第 21 页

第 3 步：使反欺诈部门成为商业决策的重要参与者

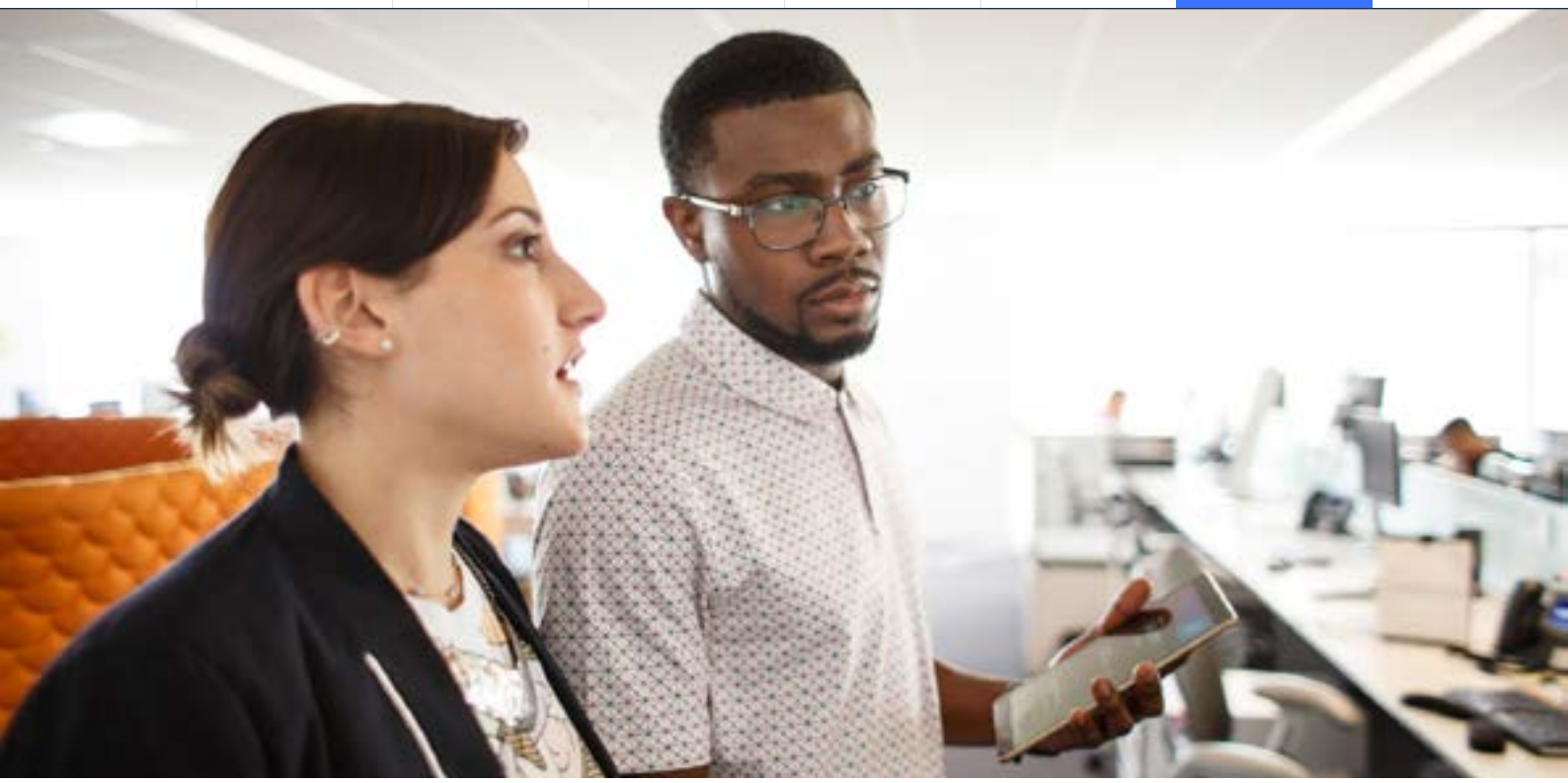
管理欺诈已不再被视为一项降低欺诈率的运营职能。

如今，反欺诈管理者越来越关注提高交易批准率、降低操作成本、支持自动化和动态应用身份验证。

他们在了解客户行为变化和重新制定销售策略方面发挥着关键作用。因此，让反欺诈团队在商业规划启动之初（而不是之后）就参与进来是很重要的。

“提升反欺诈部门的地位，使其成为整体业务的合作伙伴。从当今成功的组织身上可以看到，业务线、营销职能、财务、运营和反欺诈团队都做到了相互配合、团结协作。”

David Mattei
Aite-Novarica 战略顾问



第 4 步：制定合理的指标

确保使用适当的指标，并利用数据持续改进反欺诈策略，这有助于您增加收入。

除了欺诈损失，您还需要考虑其他指标，例如：

- 客户冒犯率（拒绝好客户 - 您可能从运营或呼叫中心团队处听说过）
- 批准率（可能来自您的业务线或运营团队）

这样您就可以从以前的经验中吸取教训，并将信息馈送到反欺诈策略中，从而帮助您最大限度提高销售额和批准率，并减少欺诈损失。

与此同时，您也能更好地衡量反欺诈团队的整体表现。

“如果商户的销售欺诈率很高，发卡方可能会变得更加严格。这样的商户在处理整体欺诈率时需要更具策略性。例如，考虑将欺诈筛查放在授权之前，以更大程度地影响授权率。”

Mark Strachan
Cybersource 全球服务总监

让团队为变革做好准备

反欺诈团队必须迅速作出反应，在疫情期间提供支持和建议。他们的角色在不断演变，新的 KPI 不断涌现。

疫情期间，无论发生什么，**欺诈者都会像往常一样积极寻找新的漏洞并加以利用**。例如：

- 转向混合工作模式可能会导致更多的上门欺诈。
- 接种疫苗的护照可能成为另一层身份，但这也会成为欺诈的热门。我们已经看到疫苗护照在暗网上以低至 12 美元[16] 的价格疯狂销售。

为下一步做好准备

重新确定受疫情影响时期的基线数据。查看订单量，考虑仍可归类为受疫情影响的订单比例。

- 为减少与授权相关的摩擦，不只是要查看撤单率，而且还要审查风险分析目标。为安全地消除购买障碍，您可以放行一定数量的欺诈行为。
- 如果您的企业计划引入新的数字功能，如 mPOS、数字签到或无接触配送（这些都可以提升客户体验），请留出足够时间评估它们可能带来的欺诈风险。

“关注新兴技术并评估其对于解决影响收入的那部分反欺诈体验的适合性。根据投资回报率和将技术应用于欺诈实践中的总拥有成本，对项目进行优先级排序。如果您还没有这么做，就应该和首席执行官协商，争取适量的资金来改善客户体验并保障收入。”

Tracy Kobeda Brown
MRC 项目与技术副总裁

16 “伪造新冠疫苗护照市场的蓬勃发展引发恐慌”，路透社，2021 年 4 月

CyberSource 的解决之道

我们的反欺诈和风险管理解决方案在阻止欺诈的同时，也同样重视接受真正的客户，因此您可以专注于自身业务。

综合运用机器学习和基于风险的策略，获得更加出色的效果

从一开始，机器学习就是我们反欺诈解决方案的核心部分，并且此后我们一直在进行升级。如今推出了 Visa 解决方案，这当中我们的实力与规模相结合，提供了相当大的优势。

- **实时自动化**根据来自 Visa 和 Cybersource 数据的情报对数百个数据点进行分析，生成强大的风险评分，可自动接受或拒绝交易，从而在欺诈者发动攻击前及时将其制止。
- **从账户登录到支付收单受理，我们可以进行自动进行风险检测，**帮助您加快完成订单并增加收入流，同时保持较低的摩擦和较高的客户满意度。

从业务中收获更多回报

运用洞察力和控制力在降低欺诈率、提高批准率和降低成本之间找到合适的平衡。

- **无法单凭一种解决方案满足所有需求**，因此我们通过多层防御（从账户冒用保护到 CyberSource Decision Manager）为您的业务保驾护航，所有这些都以机器学习的强大功能为后盾。

您准备好开始了吗？

我们可在瞬息万变的世界中为您的业务增长保驾护航。请立即联系我们了解详情。

cybersource.com

>> **点击此处**联系我们

cybersource
A Visa Solution