赢得反欺诈斗争的胜利

最有效的金融机构如何智胜欺诈犯罪分子

IBM 商业价值研究院

执行报告

银行业

IBM 银行业解决方案

企业若要从当今日益复杂、瞬息万变的环境中脱颖而出，需要改善运营状况和企业各个部门之间的协作，培养出更加卓越的领导力和更优秀的人才，管理好持续的变化并发掘根植于数据中的新的可能性。如欲了解有关 IBM 银行业解决方案的更多信息，敬请访问：ibm.com/banking。

欺诈无处不在

欺诈是最令金融机构头疼的问题，尤其在当今，电子银行业和电子支付的发展给欺诈犯罪分子提供了更加便捷的新通道，有组织的犯罪团伙借此来实施相当复杂的犯罪行为，牟取不正当利益。但是，一些领先的金融机构发现，借助与大数据和分析相关的新兴技术，实施切实有效的转型计划，可以有效抗击此类威胁。本报告将具体阐述这些机构用于抗击欺诈的最佳实践，以及有关运营转型的最佳实践。

执行摘要

对于全球大多数金融机构而言，控制金融犯罪乃是一切工作的重中之重。因此，他们会坚持不懈地开展评估，找出最佳方法，保护自己的系统、数据及客户。实际上，我们近期开展的金融欺诈调研显示，至少 80% 的金融机构每个季度都会组织管理委员会探讨欺诈和网络安全问题。

为配合开展“2015 年 IBM 金融机构反欺诈调研”，我们对 500 名银行业和金融市场高管开展了调查，这些高管的职责包括欺诈防御。为了解金融犯罪控制领域的能力现状、成功案例、挑战和最佳实践，我们还对来自世界各地的金融机构及相关行业协会的高级欺诈防御高管进行了访谈。（如欲了解有关本次调研的更多信息，请参阅*“调研方法”*部分。）

谈到当今金融机构在抗击金融犯罪时面临的挑战时，只有 56% 的受访高管认为他们的公司能够合理控制欺诈威胁。许多受访者都认为自己公司的反欺诈部门迫切需要进行彻头彻尾的改造。

许多总资产超过 3000 亿美元的大型机构均已完成或正在推进反欺诈运营流程转型。这些机构成功开发的综合业务案例极具说服力，令我们不仅看到阻止直接欺诈损失的希望，还看到了降低运营成本以及增强客户互动的可能性。这些大型机构一致认为他们至少能控制欺诈情况，52% 的受访者将这些能力视为自身独特的竞争优势。

14%

的银行高管认为自己的反欺诈能力是一种独特的竞争优势。

42%

的银行高管认为他们的反欺诈运营流程亟待彻底革新。

49%

的银行高管都在坐等客户投诉欺诈行为，或者在欺诈检测方面无能为力。

但小型公司的情况却与此大相径庭。对于总资产最多不超过 1000 亿美元的小型公司，大多数高管均认为他们处于金融犯罪危机四伏、持续恶化或十分严重的环境当中。超过 3/4 的小型公司近期未采取任何重大举措来提升自己打击金融犯罪行为的能力，同时对于这类公司，欺诈坏账在总收入中的占比出现了大幅度上升。小型公司在开发令人信服的业务案例方面遇到了更多麻烦，而且他们的现有基础技术在功能全面性与使用效率方面也都稍逊一筹。

所幸他们现在可以通过提升反欺诈与金融犯罪抗击能力来迎头赶上。与分析、大数据和高速处理相关的新兴技术可以帮助金融机构提高检测与阻断欺诈的能力，防止资金损失。这些技术还能帮助发现复杂的跨渠道欺诈模式，例如国际犯罪集团采用的组织模式。

每年高达 7000 万美元的损失难道还不足以引起您的重视?

至少 70% 的受访机构指出，仅直接欺诈坏账一项便占到他们公司总收入的 7 个基点 (b.p.) 以上。对于总资产为 1000 亿美元，年平均收入达 100 亿美元的银行而言，这意味着每年会遭受高达 7000 万美元的损失 – 并且这还只是直接损失。

如果将警报管理、调查、系统管理及客户服务等运营成本计入欺诈损失总额中，那么，银行的总损失将很容易翻一番。考虑到运营成本涵盖范围广泛，大多数受访金融机构抱怨反欺诈运营流程成本太高，投资回报率太低，也就不足为奇了；此外，42% 的受访者指出他们迫切需要实施彻头彻尾的转型，而只有半数的受访者认为他们的保护力度够强。

主要定义

- 金融机构 – 银行和金融市场公司。不包括保险公司、货币服务公司或专业支付公司。
- 金融犯罪 – 基于客户的欺诈和洗钱行为，以及以访问和盗取客户账户为目的的基于网络的数据或客户证书盗取行为。内部欺诈和总体数据盗用未包含在本次调研范围内。
- 欺诈检测 – 发现欺诈性客户交易的过程。
- 欺诈发现 – 从个人客户交易的历史记录中发现严重欺诈性行为模式的过程。

“银行原本以为尽管存在直接欺诈坏账，但一项产品总能够带来丰厚的投资回报。但是，当他们放宽欺诈成本的度量范围，将反欺诈运营考虑在内时，却会发现投资此类产品实际上是赔本的买卖。”

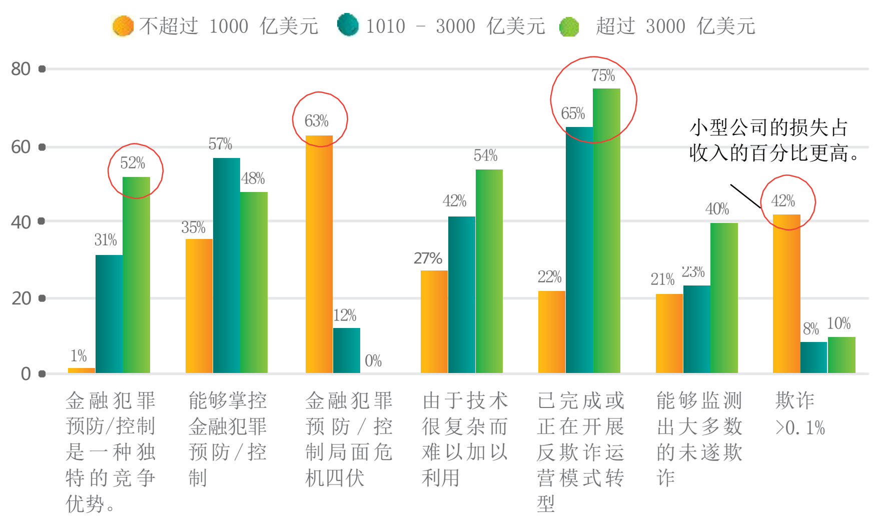
加拿大某银行的首席安全官

规模至关重要

我们发现公司规模与总体反欺诈表现之间存在一定的关联。来自大型机构（总资产超过 3000 亿美元的公司）的全部 48 名受访高管均表示他们能够控制欺诈情况，其中 52% 认为欺诈控制能力是一种独特的竞争优势。相比之下，在 315 家的受访小型公司中（总资产不超过 1000 亿美元），有 53% 指出他们所处境地是危机四伏、持续恶化或十分严重。近一半 (42%) 的小型公司表示他们的直接欺诈坏账占到了总收入的 10 个基点以上（见图 1。）

图 1

规模至关重要：小型公司感到更多威胁；而大型公司则借助转型取得良好进展



来源：2015 年 IBM 金融机构反欺诈调研。注：某些百分比因四舍五入加总不等于 100。

不同规模的机构在反欺诈方面的表现有所不同，这可能是因为大型公司拥有足够的精力和预算，能够利用最先进的大数据、分析、高速处理和信息访问技术来开展大规模转型计划。实际上，75% 的大型机构指出他们正在进行或已经完成了转型计划，而这一比例在小型公司中仅为 22%。正如我们所料，中型企业 – 总资产在 1010 到 3000 亿美元之间的机构 – 的表现处于二者之间。但是，这些中型企业似乎不甘示弱：88% 的中型企业指出他们能够控制或有效管理欺诈局面，65% 指出他们正在开展或已经完成了反欺诈运营流程转型。

有趣的是，虽然小型公司认为他们备受欺诈威胁，但有 54% 的大型受访机构表示由于难以操纵复杂技术及难以汇集整个企业的信息，导致无法检测出更复杂的欺诈行为。一家英国顶级银行的反欺诈技术主管表示：“难以管理欺诈问题的原因并不是因为我们规模太大，而是因为我们的环境太过复杂。”

“我们知道添加更多的反欺诈人手并不是问题解决之道。要想解决问题，我们需要通过培训、知识传授及良好寻源来提高现有员工的智慧工作能力。”

一家东盟银行的金融犯罪与安全部主管

强弱之别

调研数据显示，能够最有效抗击金融犯罪的机构通常规模很大，能够近实时地检测出欺诈，并且正在进行或已经完成了反欺诈运营流程转型。

通过开展基于多个因素的集群分析，包括欺诈控制程度、欺诈坏账率、运营流程转型承诺以及企业高管的支持程度等，我们将受访金融机构分为三个不同的组群，分别是：卓越领导者、高能转型者和脆弱新手。“卓越领导者”主要包括业内大型企业以及总资产在 1010 – 3000 亿美元之间的中型受访机构。“卓越领导者”的欺诈控制程度相对较高，欺诈坏账率相对较低，坚决承诺开展运营流程转型，并且企业高管对反欺诈战略工作给予鼎力支持。

“脆弱新手”主要是小型机构（其中 94% 的机构的总资产 100 – 1000 亿美元不等）。在这个组群中，大多数受访者 (84%) 均表示他们的反欺诈工作处于危机四伏与十分严重之间的状态。此外，仅 4% 的受访者认为他们的技术完备且能得到有效利用，这一比例在“卓越领导者”中高达 48%。

“高能转型者”处于上述二者之间，但同样具有鲜明的特征。在这个组群中，大多数机构 (79%) 的总资产都在 300 到 3000 亿美元之间，并且他们的总体反欺诈能力不佳（仅 8% 的受访者表示他们具备近实时检测能力，同时 73% 的受访者指出公司坏账占总收入的 7 个基点以上）。然而，“高能转型者”正在规划、正在进行或者已经完成了欺诈运营流程的转型。这个组群的另一个鲜明特征是 65% 的受访者认为他们的转型计划得到了适当融资，能够满足机构、客户及合规性要求。

决定因素

运营

以前，金融机构依赖客户致电呼叫中心质疑其信用卡账单收费问题来实现全面的欺诈检测。如今，这种情况已经一去不复返了。那时的欺诈相当简单，属于投机取巧的个别行为，例如有人不慎将信用卡遗失在了购物中心停车场，然后被其他人捡到之后疯狂购物。一家美国银行的反欺诈运营部全球主管在接受我们采访时表示，虽然信用卡从丢失之刻起到注销需要两个月的时间，但信用卡丢失率相当低，并且“损失”通常也是可以接受的。

而现在，据估计，约 80% 的消费者欺诈是有组织的犯罪团伙利用唾手可得的劳动力通过多个产品渠道在多个位置发动的短时间攻击 – 有时仅为几小时。[1] 例如，2013 年，犯罪分子在不同的时间发动了两次攻击，从 27 个国家的自动取款机中盗取了 4500 万美元，两次攻击的持续时间总和仅为短短的 10 小时。在这起事件中，犯罪分子侵入信用卡和借记卡支付处理网络，通过恶意增加账户余额，提高取款金额限制，然后将被盗的借记卡信息提供给全球各地 100 多名共犯，进行不当提款。[2]

庆幸的是，虽然有组织的犯罪变得更加有恃无恐，并且有时无法以金融欺诈为名起诉犯罪分子，但用于预防和打击金融犯罪的技术也在不断成熟。大数据和分析解决方案以及高速处理技术均取得了突破性进步，这促使“卓越领导者”与拒绝转型的企业区别开来。技术解决方案正在帮助“卓越领导者”在以下几个方面获得突出表现：

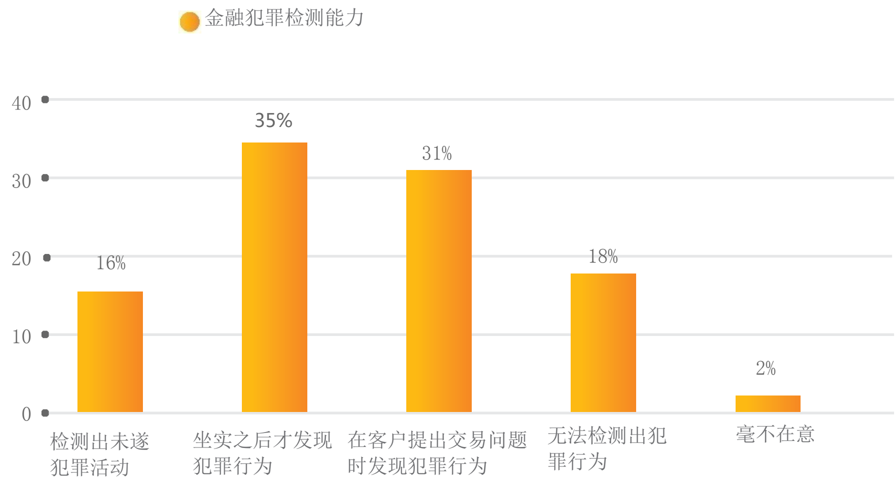
“欺诈诉讼并不是执法部门的首要任务，因此，我们最好的做法应该是阻断欺诈，而不是诉诸于法律调查和损失追回。执法部门通常只追查犯罪实施者，而不是背后真正的操纵者。”

一家美国货币中心银行的全球欺诈管理主管

- *实时检测*（在坐实之前阻断欺诈性交易的能力） – 如果能在资金被盗之前发现欺诈性交易并阻断它们，交易处理机构将能避免开展调查和追回损失，也不会给客户带来不便，双方都不会遭遇经济损失。仅 16% 的受访机构表示，检测出欺诈企图的能力是他们在抗击欺诈效力方面表现出众的关键要素（见图 2）。遗憾的是，31% 的受访者他们仍依赖于客户的交易投诉，另有 18% 的受访者表示他们无法判断欺诈方式。

图 2

大多数金融机构都是坐实之后才能检测到欺诈



来源：2015 年 IBM 金融机构反欺诈调研。

- *反欺诈和分析专业知识* – 最成功的机构会雇用兼备精深分析技能和丰富反欺诈经验的员工。虽然 69% 的受访者都在使用分析技术发现欺诈模式，但数据和统计科学家与参与反欺诈活动的员工通常处于不同部门或不同位置，两者之间相互隔离、互不沟通。因此，两个团队之间仍出现脱节现象，导致分析流程受阻。“卓越领导者”深知综合运用数据科学与防欺诈技能有助于检测变幻莫测的欺诈模式，帮助及时作出调整，防止损失发生。鉴于寻找或培养拥有多项技能的分析师相当困难，因此，许多精明的机构均已开始采用合作方式（至少将两个部门共置在一处）来增强双方互动，从而开展交叉培训。

- *集中式运营* – 许多领先机构都对同地办公理念做了进一步延伸，已开始将全企业的反欺诈和分析专业知识统统汇聚到“卓越中心”之中。这类集中式做法不仅可以汇集各类技能并提高效力，而且还能帮助规范和简化方法和技术，从而降低运营成本。谈到公司战略，一家英国银行的全球反欺诈技术主管表示：“我们正在构建一个大规模的生态中心网络，该网络包括一个欺诈分析的卓越中心和一个保存着全部警报和其他信息的集中式数据库，我们将把该网络用作一种沙箱来开展分析活动。这将能帮我们解决检测系统四分五裂的问题。”

“我们将分析和反欺诈运营人员集中在一处办公，以便他们共享观点和专业知识，提高反欺诈工作的总体效力。”

一家澳洲银行的安全性和业务连续性部门主管

- *更加广泛的信息集* – 在过去十年中，数据的数量及可用性均有显著提高，用于管理和利用信息的技术也在不断发展。在欺诈预防方面，将更多相关信息纳入分析范围，可以帮助提高欺诈检出率，降低误报率，同时降低警报管理和调查成本。然而，虽然大多数机构都使用内部交易与客户数据来分析犯罪行为，但不到半数的机构会利用来自外部来源的其他信息，仅 34% 的机构会与竞争对手共享犯罪情报。许多机构甚至都无法轻松管理自有信息。例如，受访者最常提到的一点是，他们最迫切希望能将各个领域、各个产品渠道的犯罪活动相关联，从而提高金融犯罪控制能力。实际上，组织缜密的欺诈分子经常会在一次活动中攻击多个产品渠道和机构，因此，大数据及同行间合作成为抵御犯罪的关键。

- *客户互动与客户满意度* – 领先的机构已经发现，向客户传达欺诈控制方法及开展客户互动，可以帮助显著提高反欺诈活动的效力及客户满意度。14% 的受访者表示，高效控制和预防金融犯罪的能力乃是他们公司的一项独特竞争优势；他们还指出提高客户满意度是推动公司在抵御金融犯罪方面进行投资的主导因素。那些借助更加先进的非侵入式技术来最有效地实施金融犯罪阻击计划的机构，既能做好控制工作，同时又能给客户创造便利。

技术

正如我们在上文提到的，高级大数据和分析技术的出现以及处理速度的显著提升，可以帮助金融机构抗击有组织的犯罪团伙在短时间内所发动的多渠道欺诈攻击。我们的调查揭示了一些关于利用这些技术的最佳实践：

- *多方位解决方案* – 通过访谈，我们发现成功控制金融犯罪的许多公司都在利用大量的不同控制机制，即使出现功能重叠。最成功的机构正在联合实施面向网络安全、实体解析（合作关系分析）、恶意软件检测、模式分析及实时交易评分的工具与流程。但具体到金融机构到底能同时部署多少项技术，则存在一定的局限性。一家加拿大知名银行兼管全企业欺诈事务的首席安全官表示：“我们无法面面俱到，根本不可能同时预测、发现并防御所有威胁。我们应集中精力去保护切实能够部署防御和检测工事的关节和位置。”

- *分析敏捷性* – 一个关键因素是从发现全新欺诈模式到随后调整交易评分流程来阻断此类欺诈之间的周期时间。91% 的“脆弱新手”表示仅发现欺诈模式便需四周甚至更长时间，84% 指出他们更新评分引擎至少还需要另外四周时间 – 导致总周期长达八周甚至更长。在长达八周的周期中，此类模式的欺诈将会一直存在。相比之下，24% 的“卓越领导者”表示他们可以在四周之内发现欺诈，34% 指出他们可在四周之内更新交易评分流程。

“我们无法面面俱到，根本不可能同时预测、发现并防御所有威胁。我们应集中精力去保护切实能够部署防御和检测工事的关节和位置。”

一家加拿大银行的首席安全官

我们还发现对许多机构而言，有效利用新技术均涉及到学习曲线。虽然 22% 的受访者认为他们的技术完备且能得到有效利用，但其余的受访者却表示他们的技术太过复杂（22%）、未得到有效利用（39%）或不够完备（17%）。显然，培训和平台简化非常重要。一家东盟著名银行的反欺诈和安全部门主管在解释自己所面临的问题时这样说到："我们在技术方面已经投入数百万美元，主要是我们认为能解燃眉之急的先进技术。结果，我们遇到了严重的集成问题，无法利用现有信息。"

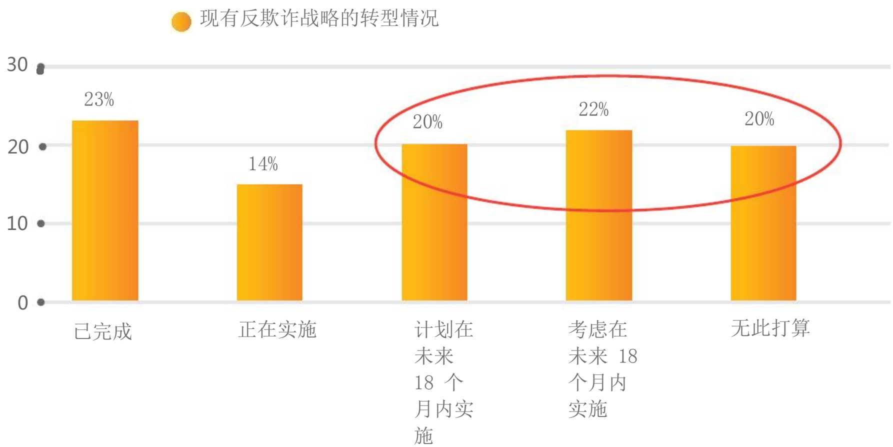
成功实现转型

大多数机构尚未开始实施反欺诈转型计划，20% 的机构根本就没有这种打算（见图 3）。受访者认为，当前阻碍转型的两个最大障碍是：成本收益比，以及优秀人才或外部顾问难以获得。

然而，当我们进行组群评估时，却发现大多数"卓越领导者"或已完成（39%）或正在执行（22%）与反欺诈运营流程和技术相关的转型计划。相对而言，"脆弱新手"在这方面十分落后（仅 9% 已完成转型计划，另有 9% 正在实施转型），甚至根本没有转型的打算（37%）。

图 3

大多数机构尚未开始实施反欺诈转型计划



来源：2015 年 IBM 金融机构反欺诈调研。

转型计划的另一个缺点在于它们的规模都很大，反欺诈流程转型也不例外。据受访者透露，在正在执行或已完成的转型计划中，大多数（85%）至少需要六个月时间，超过四分之一（28%）的转型计划需要 18 个月以上的时间才能完成。同样，在正在执行或已完成的转型计划中，64% 的计划需要花费 200 万美元以上的高昂成本。

转型计划始终需要开发强有力的业务案例才能获得有限的资金注入。虽然转型能够减少可观的直接欺诈坏账，但经常不足以抵消金融机构实施战略性计划的投资成本。已完成或正在反欺诈流程实施转型的大多数受访机构在业务案例中均从多个方面（68% 从三个或更多方面）来证明转型的意

反欺诈流程转型的最有利支持因素是客户影响和缩减运营成本的潜在机会。

义，其中最常见的一个方面是客户影响（占到 47%）。一家澳洲著名银行的金融犯罪技术主管解释说：“我们的企业文化是客户至上。我们发现，当清晰阐释反欺诈流程改进可以增强客户体验时，我们便可以得到更多高管的大力支持。”

在金融机构的成本转型业务案例中，第二个最常用的理由是降低运营成本的潜在可能。例如，高级分析技术在反欺诈领域最大的影响之一便是欺诈交易评分系统效力的提升。正如受访的一家美国一流跨国银行亲身经历的那样，妥善实施的分析解决方案可以将欺诈检出率（实报）提高 100%，同时将错误警报率（误报）降低 30%。有时候，减轻欺诈调查部门（通常是大部门）的警报处理负担可以节省大量运营成本，远远超过坏账本身的金额。

在 500 名受访者中，超过 20% 认为支持投资于阻击金融犯罪的其他证据还包括运营稳定性 (36%)、加快交易处理速度 (22%)、提高客户保留率 (33%) 以及增加收入 (29%)。

最后，与所有其他的重要投资一样，高管的支持，尤其是首席执行官 (CEO) 的支持，对于计划落地生根至关重要。一家美国著名金融机构的反欺诈运营主管发现了一个有趣的现象，他表示：“凡是转型计划得到 CEO 积极参与和鼎力支持的银行，貌似近期都曾遭遇过严重的欺诈事件。”难道这只是时间问题吗？

执行方法 – 如何成功实现转型

我们假设业务案例极具说服力，得到了 CEO 的支持，其他高管也被说服，相信提高反欺诈能力将能帮助显著提高客户满意度。那么，您能从以往的转型者身上吸取哪些经验教训呢？他们是如何通过反欺诈运营流程转型与金融犯罪作斗争的呢？哪些最佳转型策略值得借鉴？哪些策略应该规避呢？

首先，必须知道转型不是“一朝一夕”之事，这一点非常重要。如上文所述，大多数公司完成转型至少需要六个月时间（经常会更长）。此外，我们的调查还发现转型成本十分高昂。因此，在时间和成本方面制定切实可行的计划至关重要。在真正完成转型的 117 家受访机构中，47% 均采用了循序渐进的方法。经调查，我们发现了几种循序渐进的转型推进方法：

- 许多机构选择逐渐替换过时的传统系统，通常从最低效的系统开始入手。
- 一些机构首先选择应用一组简单的检测规则，随后使用规则测试及其他分析技术来逐渐完善模式与规则。
- 还有一些机构以业务部门为单位逐步实施转型。他们通常会针对每个业务部门部署相同或类似的技术平台，以避免重复系统带来的成本和复杂性。

其次，明智地选出有待改进的领域及所需功能，这可以帮助制作性价比高的业务案例及简化运营流程。一家新加坡中型银行的主管阐释了各项选择和总体战略的重要性。他说到：“在过去五到七年中，我们投入巨资构建反欺诈和安全系统，但各个系统却无法如同我们想象那般协调工作。这是因为我们只基于战术需求或特定渠道需求来选择自认为一流的技术，并未考虑到当时还不存在的全企业标准或战略。”

借鉴“卓越领导者”的经验

虽然金融机构的反欺诈能力参差不齐，但“卓越领导者”身上有许多值得我们学习的地方，包括对以下内容的使用：

- *实时检测* – 从而在造成损失及产生恢复成本之前阻断欺诈
- *敏捷分析* – 旨在快速检测出瞬息万变的犯罪行为模式
- *更广阔的信息集* – 旨在增强对每次客户交易的了解并做出更加明智的决策
- *多面防御* – 旨在预测出跨越多条渠道的复杂犯罪行为，杜绝单点故障

准备好了吗？问问您自己这些问题

- 贵公司打击金融犯罪的能力如何？
- 造成贵公司欺诈调查部门工作效率低下的原因是什么（人员还是基础架构问题）？
- 贵公司采用哪种方法来确保能够发现并阻止新兴欺诈模式？
- 要想真正在交易完成之前或造成资金损失之前阻断欺诈，贵公司需具备哪些能力？
- 贵公司如何使用分析技术来洞悉新兴欺诈模式？
- 客户对贵公司保护他们远离欺诈的能力评价如何？

更多信息

要了解有关本次 IBM 商业价值研究院调研的更多信息，请联系我们：iibv@us.ibm.com。要获取完整的研究目录，或者要订阅我们的时事通讯月刊，请访问：ibm.com/iibv

从应用商店下载免费“IBM IBV”应用，即可在手机或平板电脑上访问 IBM 商业价值研究院研究报告。

访问 IBM 商业价值研究院中国网站，免费下载研究报告：http://www-935.ibm.com/services/cn/gbs/ibv/

选对合作伙伴，驾驭多变的世界

在 IBM，我们积极与客户协作，运用业务洞察和先进的研究方法与技术，帮助他们在瞬息万变的商业环境中保持独特的竞争优势。

IBM 商业价值研究院

IBM 商业价值研究院隶属于 IBM 全球企业咨询服务部，致力于为全球高级业务主管就公共和私营领域的关键问题提供基于事实的战略洞察。

关于作者

Wilson Davis 是 IBM 全球企业咨询服务部战略、分析和反欺诈小组的副合伙人。Wilson 专门为金融服务行业提供金融和运营数据分析、反欺诈和反洗钱、直通处理、IT 部门转型及业务流程和应用系统显著改进方面的建议。Wilson 拥有达特茅斯塔克商学院工商管理硕士学位，拥有 10 年的财富 500 强企业 IT 高管经验及 15 年的合作伙伴级顾问经验。他的联络方式为：ewdavis@us.ibm.com。

David Dixon 是 IBM 分析事业部的全球金融犯罪行业主管。作为帮助金融机构制定反欺诈、反洗钱及反恐计划的全球权威专家，David 经常在国际会议上发言。在此之前，他曾领导 Norkom Technologies 及 Bearing Point 成功开发和交付业界领先的金融犯罪解决方案。David 曾在蒙特利尔银行任职十年，负责欺诈的远程监控、AML 及反恐融资工作。他的联络方式为：ddixon@ca.ibm.com。

合作者

Hester Ngo，IBM 加拿大公司分析事业部；Rick Hoehne，IBM 全球企业咨询服务部；Eric Lesser，IBM 商业价值研究院；Maribeth Mallon Haynes，IBM 分析事业部；Scott Burroughs，IBM 分析事业部；David Dixon，IBM 分析事业部；Austin Wells，IBM 分析事业部；Samiran Mukhopadhyay，IBM 销售与经销部；Angus Stewart，IBM 澳洲公司软件销售部。

调研方法

2015 年 9 月，IBM 联合牛津经济研究院开展调研，对跨国银行和金融机构开展了独立电子调查，旨在了解他们打击金融犯罪的能力。共有 500 名负责防欺诈工作的高管参与了本次调查。这些受访者来自不同地区，公司的资产规模也不尽相同。

除开展调查外，我们还对金融犯罪控制领域中领先金融机构的高级反欺诈高管以及来自相关行业协会的高管进行了访谈。我们在访谈中提问了相关问题，旨在了解他们在打击金融犯罪方面的成功经验、挑战和最佳实践以及实施的转型计划。从他们的言语中，我们发现成功的方法多种多样。

鉴于金融犯罪信息和运营实践极为敏感，通常属于公司机密，因此，无论是电子调查还是直接访谈，我们均已向受访的金融机构和个人保证不会透露他们的名称。文中的引述和统计数据都是真实的，尽管在某些情况下，我们改变了高管的头衔，以防他人直接联系他们。

注释和来源

1. “网络犯罪综合调研”，联合国毒品和犯罪问题办公室。2013 年 2 月。 https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

2. Vaughan 和 Bernard，“4500 万美元劫案告破，6 人落网”，路透社，2013 年 11 月 18 日（访问时间：2015 年 11 月 16 日）。 http://www.reuters.com/article/2013/11/18/us-usa-crime-cybercrime-idUSBRE9AH0YZ20131118#o5jDIKhY2i2 bEeV0.97

IBM Global Business
Services
Route 100
Somers, NY 10589

美国出品
2016 年 1 月

GBE03726-CNZH-02