IDC

蚂蚁集团
ANT GROUP

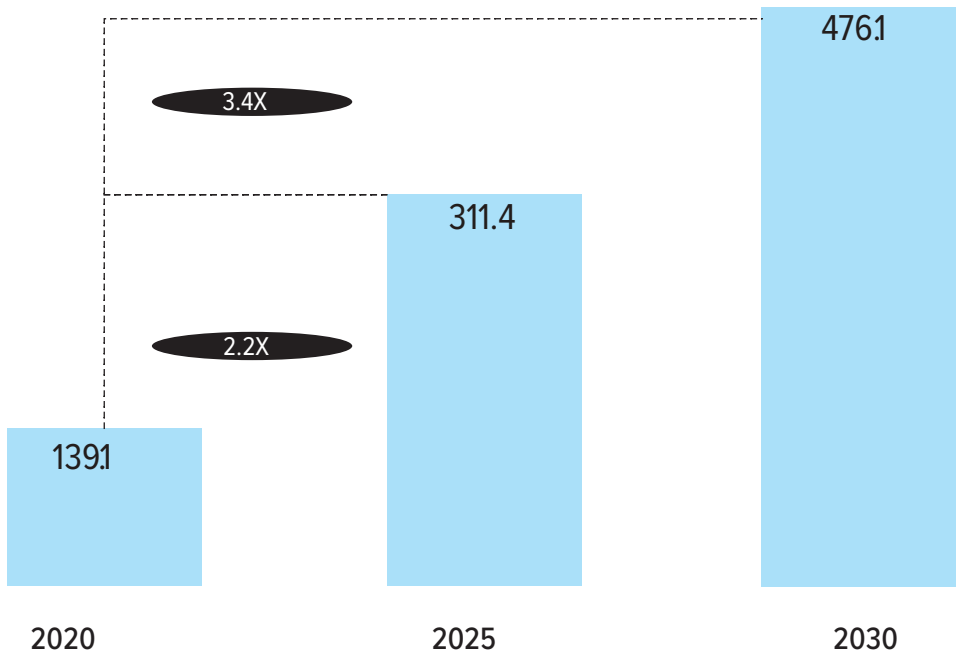
数字时代的风险博弈
十大风控技术趋势指南

在过去两年间，疫情给我们的生活带来了许多颠覆性变化。当今的商业模式已不同于往昔，随着数字化进程的进一步加快，金融机构必须要时刻为可能出现的业务风险做好准备。这也正是“IDC金融洞察”白皮书将深入探讨的议题，议题中的一个关键词，就是“风险博弈”——面对正在走向无边界和强对抗的新型重大风险，金融机构如何与之博弈，并始终领先一步？这可以说是关乎“生死存亡”的大事。

数字支付激增

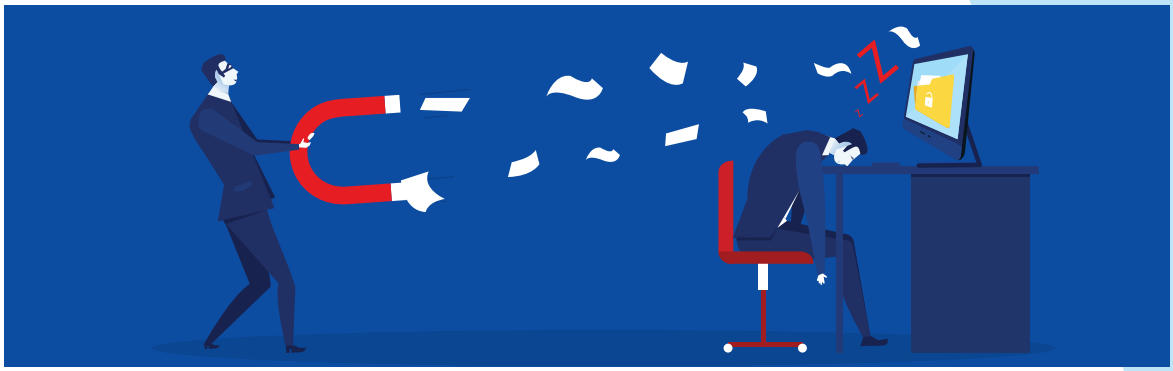
新冠疫情算得上数字化发展的一个“加速器”，但其实早在疫情出现之前，数字服务领域已经有了大规模的转型：从线上互动，到数字支付，再到依托于数字平台而生的新服务。疫情的出现加速了这一趋势，加速的势头预计将保持到2030年，届时人类早已将这次全球健康危机甩在身后。图1数据显示，2020年到2025年，全球消费者数字支付市场预计增长2.2倍，而在2025到2030年期间，上涨幅度预计将进一步增至3.4倍。

图1 全球消费者数字支付市场 （万亿美元）



来源： IDC金融洞察，2021

数字化与金融风险相生相伴



数字化世界的机遇和潜力巨大，但也充满了风险。随着企业加速运营调整以应对数字化进程，这种激增的趋势带来了明显的合规风险和业务风险。

更多的合规要求

与数字支付兴起密不可分的，是大量出台的监管规则，尤其是与安全保障和用户体验相关的区域性标准。企业必须充分认识到各类利益相关方、金融机构、供应商及合作伙伴的要求，确保自身合乎规范、政府监管要求及标准。

各机构都必须面对这一现实：数字化即意味着更多的合规要求。在澳大利亚，四大银行50%的技术投资都用在了合规方面，据称是为了让自身为迎接数字化世界做好充分准备。其中的重点投资领域包括风险报告、网络安全与环境、身份验证、反洗钱和打击恐怖主义融资合规、支付诈骗等。在亚太其他地区，各机构也在合规方面进行了大规模的投资。

另一个毋庸置疑的现实是不利事件出现的越多，监管就会越严格。例如，一旦出现停工和服务不可用的情况，为了增加业务的连续性，监管必然就会出台额外的措施；而当出现网络安全事件时，网络风险的管控就会进一步升级。为了应对欺诈的挑战，全球范围内将出现一系列更完善的监管举措，包括对合作伙伴的尽职调查、向监管机构进行事件报告、向受影响的消费者公开诈骗案件的细节等。

IDC预测，到2025年，85%的零售商都将提供至少两种无接触式的支付方式，进而将转化率和客户保留率分别推高40%和30%。

（#IDC Asia -Pacific Payment Future Scape prAP47554121）

支付渠道、平台和功能一时泛滥

当下零售商和商家都在急于找到合适的渠道，以满足消费者不断变化的偏好。理想情况下，企业需要为不同渠道提供不同的分配商品和服务的选择（网络、移动App、数字平台等），为消费者提供不同的交易方式（支付类型、传统销售点、移动钱包、实时支付等），还有一系列其他可以改进数字体验的功能（自动推荐、忠诚度积分、先买后付等）。

这种对选择的追求很容易拉高服务成本。随着服务消费者所花费的资源越来越多，可以预见，未来将出现一大堆的工具来确保交易的安全、可靠和便捷性，包含从认证到下单的方方面面。

在之后的章节中，我们会讨论到各类欺诈问题。随着渠道的日渐增多，许多的风险因素会在数字交易和支付过程中发挥作用。相应的，这些风险因素作为载体和媒介，也会衍生出许多的欺诈风险。我们也会探讨跨渠道、跨平台式的欺诈是如何实现的，并重点关注欺诈犯如何通过不同的渠道、支付类型和功能实现诈骗手段的不断升级。

同时，在追求选择多样化的过程中，为了向消费者提供便捷、安全和可靠性，出现了大量效率低下的解决方案。

来自第三方的风险

当前，由于金融服务和其他非银行的生态系统相互交融，金融机构不得不面对第三方的风险问题——使用第三方提供的数据、基础设施、服务和软件相关的外部风险。随着开放式银行的兴起，第三方风险逐渐成为一个金融机构需要考虑应对的难题；此外，在进行生态合作和平台建设时，银行在与数据供应商、云服务供应商和潜在伙伴的合作过程中，也需要慎重考虑这一点。由此，像隐私保护多方计算这类解决方案就应运而生，我们在之后的章节中也会提到这一点。

另外一个重要的问题即身份管理。越多的渠道和平台融合在一起为消费者提供基于生态系统的解决方案，确保账户或持有人身份信息不被泄露就变得越重要。此外，确保第三方的身份没有问题，以及确保消费者在被授权的情况下获得金融数据、进行交易、从账户进行支付也显得愈加重要。

如果不对AI风险加以管控，AI风险可能对业务产生严重影响

随着人工智能（AI）和机器学习（ML）逐渐成为最重要的支持风险管理的技术，金融服务供应商必须做好应对由AI及其发展所带来的各种新风险。

与AI相关的风险不仅包括操作的风险，还包括针对AI弱点的诸多风险，比如由于数据投毒而导致的模型风险、由于缺乏可解释性和偏见而导致输出模型不可靠的风险、由于数据泄露而导致的隐私泄露风险等。

在尚未建立完善的AI风险管控框架的情况下采用AI和ML技术，对于任何企业来说都是非常危险的。

应对措施越来越复杂

为了有效地应对各种场景下的欺诈，零售商和商家都急于将各类渠道、业务流程、工具和技术放到一起，越来越多的解决方案应运而生。这意味着组织内部会出现更多数据孤岛、系统孤岛甚至是业务孤岛。当存在孤岛时，风险、IT、欺诈和运营之间会愈加缺乏协调性，迅速风险监测和及时有效应对的能力也会下降。

另外，数字互动和数字支付的急剧增长推动业务加速数字化转型——从售前到支付，再到售后。然而，在大多数情况下，这些改进让系统和流程变得更加复杂。随着时间的推移，这些本就因传统架构和技术缺乏而备受困扰的企业，在应对新型风险时会显得愈加困难。由于对解决方案的需求只增不减，与第三方结成合作伙伴和组成同盟成为金融机构必然的选择。

然而所有这些为了应对需求的变化，企业将付出更高的成本。为了确保资金在不同网络环境间转移时的无缝体验，企业会在支付网关、设备、软件和基础设施方面加大投资。商家无论规模大小，都必须对技术投资做出规划，以维持不同的商业模式来服务不同的消费者群体以及应对其行为上的变化。但是，对于大多数企业而言，提供跨渠道、跨分销网络且快速周转的无缝支付体验的成本是非常高昂的。

由于传统系统的存在，企业为了适应数字化趋势所做的努力更多地是在现有架构上增加更多的层次。结果，这也导致许多低效的结果显现，其中之一就是企业内部对风险数据的决策不一致。数据孤岛越普遍，精准的决策变得越来越困难。因此，各组织必须实时对风险威胁和影响进行监测和评估。

面对更多的消费者不确定性

大多数数字支付的新用户都发现，在得以完成交易之前，要接受条款的流程很强制化且不易理解，这从很大程度上降低了消费者对数字化的信任感。另外，日益提升的数据安全和隐私保护意识，也让消费者对数字化支付的安全性产生了不确定感。在中国，个人信息保护的相关制度在《网络安全法》就已经有了专章规定，其后的《民法典》人格权编和《数据安全法》也先后规定了涉及个人信息的具体保护制度和相关要求——数据应当在客户的控制下保持隐私性，且客户应对数据的访问权限拥有控制权。这就需要企业建立一个可访问的安全架构，仅向被授权的可信任的第三方（TTP）开放，且需经过严格的安全控制。即便没有这些强制性的文件，客户也会要求同等的数据可访问性和安全性，如果企业做不到这一点，那将面临失去客户的风险。

当不信任危机出现时，企业都会收到大量客诉，一旦消费者对交易的安全性产生不确定情绪，客户满意度下滑，消费者放弃交易，收入增长随即成为泡影。随着不确定情绪的泛滥，企业的整体业务将面临巨大的挑战。

值得关注的欺诈趋势及欺诈风险的新特点

近年来，数字支付面临的欺诈风险呈上升趋势，由于很多企业急于开展数字服务、实现数字支付，以致在系统内部和业务流程上留下了许多隐患，让黑产有机可乘。IDC的一项研究表明，相较于2020年，在2021年，亚太地区52%的企业因遭遇诈骗而蒙受的损失上涨了至少5%，26%的企业损失上涨了至少11%。由于支付管控不利及降低风险手段的不到位，欺诈活动现在越来越猖獗。更糟糕的是，黑灰产的欺诈手法正在不断升级，欺诈套路也变得越来越复杂。

哪些威胁正在变得愈加常见？欺诈风险又是如何演变的呢？

身份欺诈

通过“半真实半虚构”的信息做成的假身份，通常被称为“合成身份”，这些身份信息可以用来进行借记卡/信用卡诈骗，或者开通假账户等，成为消费者群体易受攻击的薄弱之处。根据IDC报告（# IDC #US46690220），20%的消费者贷款和信用卡扣款都是由合成身份欺诈造成的。单就美国而言，因合成身份而导致的扣款总数额可能就远超100亿美元。由于合成身份中混入了大量的真实数据，传统的反欺诈工具模型不足以检测并验证这些基于多重数据的参数。

2020年，美国的联邦贸易委员会报告称，民众投诉的数量上涨了45%，其中大多数都是由于身份欺诈引起的。相较于2019年，这一数字上升了113%。

（来源：iii.org）

合成身份欺诈会让零售商和金融服务供应商蒙受巨大的损失，这类欺诈行为不仅很难被发现，而且可能还需耗费大量的时间来弥补造成的损失。

对于那些没有统一公民身份和国家ID数据库的国家来说，身份欺诈的问题尤其值得关注。由于新用户在开户时无法实现卡证比对，使身份欺诈成为高发风险。但是现在，在生物识别、OCR、人工智能等技术的支持下，KYC环节可以在远程实现。对金融机构来说，建立准确的客户档案是安全合规的风险防范的基础。

新交易类型中的风险

根据IDC报告《IDC FutureScape：2022年全球金融服务及支付预测》，到2023年，高达65%的各渠道消费者将会尝试即时的金融服务。这说明了，消费者的购买周期中享有多种不同的金融和支付选择，这也为欺诈的发生提供了新的土壤。

其中，“先买后付”的支付方式在线上渠道越来越受欢迎。该方法主要是为了帮助商家在消费者购物时提高其客户留存与转化率。随着疫情的发展，消费者们越来越倾向于线上采购，因此商家和贷款机构开始合作推出不同的机制，例如“先买后付”来帮助消费者完成交易。在澳大利亚，“先买后付”的服务发展迅速，成为了一种在客户流向竞争对手之前，能够留住他们的有回报且有效的手段。尽管“先买后付”的模式还处于起步阶段，黑灰产还是看到了新的“机遇”，他们快速设定了针对新交易方式的诈骗手段，包括但不限于先买后付、微贷款、购后保险、忠诚度积分兑换，甚至是数字货币等等。

根据澳大利亚证券交易所（ASX）的股票表现，“先买后付”板块的交易额在2019/20年度增长了55%；但是，与“先买后付”相关的欺诈投诉相较于2019年也几乎翻倍。

欺诈和洗钱逐渐呈现结构化趋势

事后警方怀疑是第三方的电商平台泄露了相关的客户数据。由于涉及的金额较小，传统的反欺诈风险手段未能被触发。尽管从事后来看，涉案账户数量庞大，总金额也是相当惊人。这种小额多笔的犯罪方式在洗钱中也很常见，通过不引人注目的小金额进行洗钱操作被叫做“结构化洗钱”或“拆分洗钱”。

2021年10月，在泰国近40,000名信用卡和借记卡的持卡人上报了至少1000万泰铢的损失，作案人是在泰国的一个诈骗团伙。

欺诈向多渠道、跨渠道的方向发展

这种欺诈类型的风险在于他们的非法活动各不相同，在源头上很难被察觉。黑灰产会通过移动漏洞或第三方系统的漏洞获得用户数据，随着越来越多这样的数据暴露，欺诈分子骗取消费者的套路也变得越来越难防范。

诈骗活动也开始针对各种新兴的渠道和设备展开。当金融或支付机构在努力适应新渠道的时候，新型诈骗案件的数量也在不断增加。这些新的威胁一般不会引起人们的警觉，因为无法与一系列已知的威胁相提并论。银行和不法分子之间的诈骗检测和防范，就像猫鼠游戏一样充满变数，商家需要基于不断升级的技术完成对交易的风险检测和防控，与此同时，不法分子也在无时无刻、毫不留情地寻找着新漏洞。

在这里，另外一个重要的概念就是如何将支付一体化融入到消费者服务中。在亚太地区，社交媒体生态中发酵的“共享经济”相关支付活动给商家带来了许多商业机遇。共享经济和社交媒体的

2021年9月，多家银行的75名客户遭遇欺诈交易，共蒙受了近50万美元的损失。诈骗分子通过把短信验证码（OTP）转移到海外的移动设备上，成功实施了诈骗活动。此类案件之所以能够发生，是因为诈骗分子可以在未被授权的情况下访问海外的电信运营商。

（来源：ChannelNewsAsia）

融合产生了新的客户群体，他们使用的新的支付方式支撑起了一个由服务供应商、社交媒体网站、零售和货运公司、金融服务供应商构成的生态系统。由于交易需要在社交媒体平台上发起和完成，社交媒体供应商不得不在应用内部提供独立的或与他人合作的支付解决方案。重点是，随着新支付平台的出现，人们也需研究确保其交易和支付安全的新方法，包括认证、加密到威胁管理等。

电信网络诈骗风险趋于专业化和团伙化

电信网络诈骗作为一种相对新颖但是形式多样的欺诈手段，即便企业有欺诈风险管控体系，它仍然造成了严重的影响。越来越多的消费者被盯上，成为电信网络诈骗的受害者。在这些诈骗案件中，不法分子通过欺骗和心理操控诱导，促使受害人本人向不法团伙控制的账户进行汇款操作。截至2020年，有约41%的企业报告其曾遭遇过本人操作的诈骗赔付申请，而随着数字化趋势的进一步发展，这一数字无疑将会继续上升。根据UKFinance的报告，英国在2021年上半年共报告了将近7.539亿英镑的损失，其中大部分案件都与电信网络诈骗（APP Fraud）相关。这进一步印证了一个事实，黑灰产正在逐渐超越传统的作案手段，迭代升级。

根据新加坡最新的警方通报，2021年上半年，新加坡报告的诈骗案件中有40%都与电信网络诈骗相关。前十大欺诈类型造成的总损失高达1.25亿美元，而2020年同期这一数据还不到5000万美元。

领先一步：
风险应对的基本原则

欺诈本身的性质及随之而来的商业风险都在不断地发生变化，让不少用户深受其害，影响十分恶劣。随着新的欺诈手段和形式的不断涌现， 其影响会更加深远。未来，可以预见的是数字互动会越来越多，企业也将面临更复杂的业务形态。

至于影响的范围、问题的规模以及具体对业务会产生何种影响，目前还尚未有明确的定论。然而，可以明确的是，企业若想在数字化世界里生存下去，安全布局必须走在风险之前。

01 面对日益复杂的欺诈手段，不断升级新的解决方案

诈骗分子和犯罪团伙不断在寻找着企业网络和系统的薄弱之处，利用从多种来源（社交平台、用户数据库、邮箱地址等）收集到的信息来确定用户的真实身份，并制定相应的计划来拦截合法交易，或创造条件诱使用户进行非法交易。由于黑灰产可以保持匿名行动，且技术成本较低，他们甚至可以突破地域的限制，实施跨国网络犯罪。这些作案团伙通过工于心计的诈骗套路突破消费者的精神和心理防线，而这些手段隐蔽，往往是传统的欺诈检测工具所探测不到的，面对各种新的风险，那些传统的工具已经落伍。最好的欺诈管理解决方案，需要与时俱进。





02 用系统性工具作战

由于历史原因，许多机构会有数个欺诈检测平台，通常部署在产品层面，导致不同领域之间的数据孤岛问题，容易被欺诈者利用。为确保能有效应对所有类型的风险，企业必须研制系统性的解决方案，涵盖风险的威胁感知、检测、处理和分析。这些解决方案不能只是应对单个问题的独立方案，更应该是系统性的。

03 合作与协作

大多数的中小企业、商家和零售店都受限于能力问题而“各自为政”，当数字化机遇到来，很多公司都没能独立制定一套有效的机制。因此，企业依赖于建立合作关系，以此提高安全水位。当合作和一体化的程度提高，我们就能更容易地对潜在的新型欺诈活动进行更快速、更高效的侦别和分析。

从行业的层面来看，在抵抗各类风险的过程中，互联网公司、运营商、银行及支付机构，都能够从不同维度感知到风险行为，并依据自身的数据和风控能力基础，开展独立对抗。由于缺乏数据流通的基本框架，各方之间未能形成有效的数据和科技能力方面的合力。为了更高效、更精准的应对数字风险，行业协作势在必行。

04 在欺诈活动相互关联的世界里，以团体形式与之对抗

数字“互联”正在成为一种流行的商业运营模式，在追求数字化的过程中，企业对其产品及服务会进行解绑和再捆绑，进而创造新的价值链和生态系统，为消费者提供更完善的服务和体验。这种以生态系统为导向的模式要求不同的系统供应商之间相互开放、互联，以确保商品和服务能够实现无缝交付。但与此同时，这也会大大增加使商家暴露在新型威胁之下的几率，新型威胁的蔓延速度更快，受其影响的用户、渠道、网络、生态系统技术平台数量会更多，多个企业同时暴露于威胁之下的风险也将随之增加。在此情境下，欺诈攻击往往影响的是多方，在生态系统中形成“多米诺”效应，先是金融科技公司，再是支付服务供应商、数字钱包和新型银行等。毕竟，这些供应商都在积极建设平台，以实现多方交易。更甚者，在跨境支付欺诈案件中，不同地方法规、机构检查、系统和司法的差异会让欺诈调查变得更加复杂。

鉴于欺诈案件相互关联的本质，我们亟需团体性的解决方案，实现数据、威胁情报、最佳实践和应对措施的共享，进而让整个生态系统获益。只有个体安全了，整体才会安全。

05 教育用户

除升级技术之外，提高用户的风险意识也非常重要。步入数字化时代，很多用户也都是第一次直面线上欺诈的威胁。这个群体是欺诈链条上最最薄弱的一环，因为当他们放下戒心进行交易的时候，欺诈风险才会趁机滋生。因此，许多组织会提前提醒用户注意鉴别和防范潜在的风险。

值得关注的十大新技术能力

面对快速变化的欺诈发展形势，传统降低风险的做法和欺诈检测工具是否能及时应对？如果不考虑采用新的工具和技术，企业是否能够安然地扩大其数字化业务的规模？现有的基础设施是否能够支撑企业分析海量数据、检测欺诈，尤其是新型欺诈？对于亚太地区的银行、商家、支付公司和其他金融机构来说，这些问题的答案可能都是否定的——面对数字化世界中不断涌现的新威胁，他们可以说是处于劣势。在本节中，我们将重点说明十项科技趋势，凭借这些能力，金融机构才能够有机会实现可信的智能黑灰产对抗（见图2）。

图2 2022年
欺诈管理领域值得关注的十大能力

01

人工智能，
风控能力提升的基础

02

威胁情报的挖掘技术，为风险防控提供有效依据

03

全图风控，实现动态可视事实风险挖掘

04

高效的算力体系，为精准流畅风险防控提供算力支撑

05

极速风控，实现更快的实时风险决策

06

主动式风控，在即时响应基础上主动出击

07

端云协同，提高计算效能保护用户隐私

08

多方风控，确保安全的跨机构协作

09

可信AI，智能风控系统的安全基础

10

用户行为分析（UBA），将变得愈加重要

来源：IDC金融洞察，2021

根据IDC全球人工智能行业应用调研，银行在以人工智能为中心的新型平台方面的支出大幅增长，从2022年到2025年，该类支出年复合增长率约为22%，到2025年将达到280亿美元。

01 人工智能，风控能力提升的基础

预计到2025年，银行业还将再投入约310亿美元用于在现有系统中嵌入人工智能技术。在接受调查的100位来自全球银行业的高管中，多数人表示他们会将欺诈管理作为重点，其中，有些银行在与欺诈相关的场景用例中已经应用了人工智能，包括开户欺诈（57%）、支付欺诈检测（57%）、欺诈操作和调查，（53%）还有反洗钱监测（46%）。自2022年开始，人工智能将成为打击欺诈活动的一个重要基础能力，人工智能将有效缩短决策时间，在7*24小时的全天候业务中，帮助实现客户快捷、无缝的交易体验，同时确保决策的准确性。

02 威胁情报的挖掘技术，为风险防控提供有效依据

IT安全解决方案不胜枚举，而市场仍然对多种威胁情报有强烈需求。因此基于巡检技术的威胁情报挖掘和分享能够持续为金融机构提供与新型威胁、欺诈迹象相关的信息。金融机构需要对这些情报进行审查，同时记录不同威胁情报效率和准确度得分，以便更好地了解不同的线索，进而指导对各种威胁的检测、识别、调查和处理。

黑灰产通常不会只在一个平台犯案，因此威胁情报对金融机构来说至关重要，例如亚太地区的许多银行协会，他们会定期分享他们感知到的威胁情报，并和行业分享应对举措。对金融机构来说，你得到的情报越多越准确，就越有可能在风险防控中领先于黑灰产。

03 全图风控，实现动态可视事实风险挖掘

金融风险决策是一个不断对抗升级的过程，从单一事件和孤立行为来分析无法获得准确决策。随着大规模图计算技术的发展，风险防控将从单一时间切片的图数据，走向基于时序的图数据，该防控方式将有效沉淀如账户盗用、电信网络诈骗、套利等风险特征，通过知识表征推理发现更多稀薄关系和隐藏风险，结合规则推理、规则挖掘与规则学习挖掘更多风险模式并有效泛化，让风险知识和实时交易事件联动实现动态图推理，形成全局的洞察，构建实时监控体系。基于大规模图技术的全图风控能够支持千亿级的金融风险知识图谱，进而为管理者们提供全面、可见、动态、实时的交易风险概览，使他们能够监测风险并及时决策。

04 高效的算力体系，为精准流畅风险防控提供算力支撑

交易和互动的数量、频率都在急剧增长，随之而来的是数据的激增，企业几乎要被海量的数据所淹没。此外，消费者设备、支付渠道、5G网络、物联网等也在不断产生新的数据。现在，企业所面临的挑战是通过分析从不同来源（结构化和非结构化）收集到的数据，从而发现欺诈的线索。然而，生成的大量数据可能会使存储和处理的环节负担过重，进而让不法分子有机可乘，组织比如跨境洗钱、非法交易等网络犯罪。一旦处理和分析数据的机制存在缺陷的话，那么虚假交易的中间人就很可能“隐身”其中，为了能够实时、准确地检测到欺诈行为，只有将传统的架构转为云计算和多节点高效算力体系，才能利用更高的计算效率来支撑人工智能/机器学习的计算需求。

05 极速风控，实现更快的实时风险决策

欺诈检测的实效性对金融机构来说至关重要，分析决策环节的每一秒延时都会降低用户体验，也让金融机构和用户增加一份资损的风险。在登录、交易支付、验证检查或用户验证等环节，实时决策的能力有赖于风险情报的收集和风控系统强大的分析和计算能力，而如何解决大规模风险数据计算中的耗时问题是行业面临的一大挑战。极速风控通过预测的方式将风险识别和风险决策进行解耦，通过提前风险计算，提高决策时的风险判断效率，实现毫秒级的实时风险决策。

06 主动式风控，在即时响应基础上主动出击

传统的风险管理解决方案大都是被动的“事后应对”：即在不利事件发生后，基于已有信息做出判断，采取保护性行动，以便之后能够及时应对类似的攻击。但这还远远不够，尤其是面对技术越来越好、作案手段不断演进的欺诈团伙。随着人工智能及其相关技术的发展，企业主动应对潜在的风险变得可能，例如通过主动和用户产生交互，来获得更多的风险信息，帮助平台做更好的风险判断，同时给到用户更好的安全服务。以本人授权的被诈骗支付为例，传统的风险管理系统仅能在检测到风险后限制或冻结交易；而现在，系统能够在发现潜在风险后，以图文提示、电话等多模态交互方式进一步确认风险，提醒用户主动意识到欺诈风险。

IDC预测，到2023年，50%的新基础设施都将部署在边缘。

(#IDC Doc # US48242421)

07 端云协同，提高计算效能保护用户隐私

随着企业越来越重视隐私保护和用户体验，传统的风险防控将面临全新的挑战，为了应对隐私保护和用户体验的挑战，端云协同的方案应运而生。受海量流媒体数据的驱动，企业需要让数据处理环节更靠近数据的来源，以进一步降低延迟、加快决策，减少个人数据的传输。通过端云协同的风控方案，企业可以让隐私数据计算在用户智能终端（如手机）中进行，将不含隐私信息的决策结果输送到云端，以实现“端云协同”的风控保障。

08 多方风控，确保安全的跨机构协作

数字化世界愈加互联互通，但很多时候，即使一家公司内的风险数据都没有被整合，更不用说行业间风险数据的互联互通。基于此，多方风控技术已在广泛试点使用，不但让多方在共同应对欺诈时实现数据、模型和分析结果的共享，而无需牺牲数据隐私或数据集的质量。有了这一更高效的协作方式，多方均可提升自身在鉴别和应对风险方面的能力。多方风控主要由区块链及隐私计算技术支撑，比如可信执行环境（TEE），多方安全计算和联邦学习，使得不同的机构能够在数据隐私得到极好保护的前提下进行风险数据共享，甚至联合建模。因此，为应对连通性风险，各商家、银行和第三方支付机构之间的“互联互通”十分必要，同时，还须保证这种“互联互通”的安全性。详见IDC关于多方计算的报告（《注重隐私保护的计算确保了开放金融所需的平衡》，2021年7月，IDC Perspective-Doc #AP47796421）。

09 可信AI，智能风控系统的安全基础

人工智能（AI）的应用是风险管理中出现的新常态。但是，AI不仅仅可以为好人所用，也可以被黑灰产作为突破口，或者攻击武器。由于风险防控是一场和犯罪团伙的竞速赛，企业必须开始考虑他们以人工智能驱动的风险防控系统是否足够稳健、可靠，能够扛得住黑灰产的攻击。这时对抗智能就变得尤为重要，它建立在经济学的博弈论框架之上，通过模拟攻击者和防御者之间的冲突，让机器自动且实时、动态地对自身系统进行安全性攻击，从而提升模型能力，使模型更加鲁棒（robust），处理结果更加准确。先进的欺诈管理解决方案已经采用了对抗智能技术，以提升人工智能模型的稳健性，此涉及的技术很多，包括像防御性的对抗性权重扰动（AWP）、投影梯度下降（PGD）等概念和技术。

同时，随着AI技术被更广泛地应用于数字化业务风险管理中，AI本身的风险也值得人们更加关注。这其中，包括AI的运营风险、AI决策的公平性和可解释性等，这些也是很多企业在扩大其智能数字化规模时面临的新问题。

在智能数字化服务中，我们必须尽可能地严格看待人工智能/机器学习模型所做出的决策。如果人工智能/机器学习的决策是基于不完整、低质量、非客观的数据集，通过错误的建模方式和错误的变量集而做出的，在未来可能会引发了诸多争议。因此，企业应当建立一个值得信赖、可靠且可追溯的AI安全框架，来更好地管理AI相关风险。尽管AI构成了应对复杂欺诈案件的解决方案，但如果没有恰当的AI治理框架，AI也可能会影响用户体验甚至是破坏品牌声誉。AI模型的安全性也需要保护，因为它们也可能会被那些有技术团队的专业作案团伙所破坏。

10 用户行为分析（UBA），将变得愈加重要

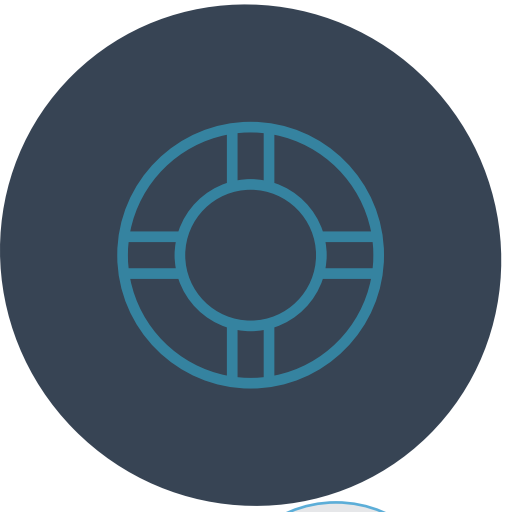
金融机构在行为分析方面的投资正在逐年增加，以提升其分析客户资料、互动模式和交易数据的能力，此外，行为分析还能帮助银行发现可疑活动，检测和预防欺诈。多年以来，在IT安全市场上，人们都是在不利事件发生后才想起这一能力，因而直到现在，UBA的相关投资仍相对缺乏；但是，未来对UBA的投资估计不会小。当然，分析的本质决定了对其投入的时间越多，效率越会提升。要想实现有效的UBA，需要花费大量的时间并进行多次的细微调整，同时还需制定一条恰当的路线图。随着时间的推移，企业使用UBA会愈加成熟，逐渐形成自己的反馈回路并获得一系列的结果，根据这些结果，他们可以再进行建模。

参考案例：TNG Digital

那些身处抗击诈骗一线的人

马来西亚的数字交易正在兴起，TNG Digital 身处这一浪潮的前沿与中心地带。TNG Digital 隶属于大马一触即通集团，由联昌国际银行、蚂蚁集团及纽约投资公司Bow Wave Capital共同所有。TNG Digital见证了马来西亚数字化的爆炸式发展，其旗下市场领先的一触即通钱包也迎合并引领着这一趋势。

一触即通卡起初通过支付过路费和停车费的预存卡而被人们所熟知，之后，它利用自身金融科技方面的声誉，推出了“一触即通钱包”，服务于近1600万用户——差不多占到了马来西亚人口的一半。该钱包不仅可用于零售和电子商务的日常支付，还可用于娱乐、旅游及其他的生活服务消费。



一触即通钱包的用户数量还在持续增加。“首席风险官Teh Huey Tzi表示，在新冠疫情逐渐蔓延全球的大背景下，该钱包的用户数量出现了显著的增长。她告诉我们，“政府正在通过向市民和用户发放补贴的方式来鼓励大家使用电子钱包。”在马来西亚，政府推出了ePenjana、 eTunai、eBelia等项目。只要用户注册了项目选定的一些数字钱包，即可获得高达100林吉特（约合23美元）的奖励，可在和当地商户的首次交易中使用；此外，政府还推出了推动线上商户使用电子钱包的计划，鼓励商家通过数字平台提供产品和服务，并在这些平台上接受数字支付（比如电子钱包）。

当然，这一趋势不只出现在马来西亚。Teh表示，目前东南亚75%的消费者实际都在线上，2021年，就有超过1600多万的消费者转移到了数字平台上。“可以预见，这一趋势将继续蓬勃发展下去，”Teh说。另外，她还提到了商户线上销售额的急剧增长，“在未来5年内，80%的商户都预测他们将有超过一半的销售额来自线上订单。”

首席风险官Teh Huey Tzi表示，在新冠疫情逐渐蔓延全球的大背景下，该钱包的用户数量出现了显著的增长。她告诉我们，“政府正在通过向市民和用户发放补贴的方式来鼓励大家使用电子钱包。”

与数字化趋势快速发展相伴而来的，还有欺诈、网络安全等不利事件。Teh表示，TnG正在努力学习以鉴别多样的欺诈模式，包括使用卡片支付（借记卡和信用卡）的欺诈。“今年以来，黑灰产的网络欺诈活动愈加猖狂，消费者往往被诱导向由犯罪分子控制的账户付款，比较常用欺诈手段包括电话、短信、邮件、假冒网站、社交媒体发帖等。”她解释道，“实际上，犯罪分子要的是让人们交出自己的个人信息和密码，之后再利用这些信息说服消费者授权支付。现在，冒充不同身份进行诈骗的案件越来越多，比如犯罪分子会冒充银行、政府机关、警察局、投资机构甚至是医疗机构的工作人员来实施欺诈。所有这些骗局都有一个共同点，那就是线上平台，通过搜索引擎、社交网站和虚假网站进行广告投放。”

TNG Digital的目标之一就是推出“马来西亚最便捷的电子钱包。”Teh表示，要做到这一点，就必须在打击欺诈活动和优化消费者体验之间找到一个平衡。对于消费者来说，繁琐的认证和验证步骤可能会令人失去耐心。不管是对于TNG Digital还是对于其他数字化企业来说，如果不能在两者间找到平衡，那么它反而会成为一个商业风险点。“用户可以直接掏出钱包来用现金支付，那么你可能也就此失去这个用户了。因此，我们需要在防欺诈和流畅的用户体验中间找到一个平衡点，”Teh表示。

Teh表示“现在，很多企业都非常关注频繁出现的欺诈攻击问题。但与此同时，企业也希望能简化结账的步骤。

为了预防欺诈，TNG Digital的风险团队使用了一系列的工具。“TNG Digital对先进的安全系统进行了大量投资，包括实时交易分析、对比设备参数以分析用户行为等。我们还对全新的欺诈探测和筛选工具进行持续优化，这将帮助我们进一步防止欺诈。我们现有的安全功能包括6位安全码、一次性动态密码、多重要素验证、3DS验证、面部生物识别验证等。我们的面部识别技术是由Zoloz支持的。”

Teh还补充，“我们有人工智能、机器学习和多种规则模型，模型经过一群训练有素的欺诈管理人才的人工干预。系统会将可疑的行为模式记录下来，并不断地与用户账户的活动日志做比较，一旦发现不寻常的活动，包括不同的用户登录，即可直接锁定可疑的欺诈行为。”

除了对技术的广泛应用，Teh和她的团队也深知专家的参与至为关键。“归根结底，问题在于我们拥有多少资源。”重点不在于团队中人员的数量，而是技能和工具的质量。

“我的团队人数一般，但是针对我们现有的业务规模来说，是完全够用且可以管理的，我们的很多人才来自于我们的合作伙伴蚂蚁集团的培训，因此有能力从不同的角度看待发生的各种欺诈案例。”

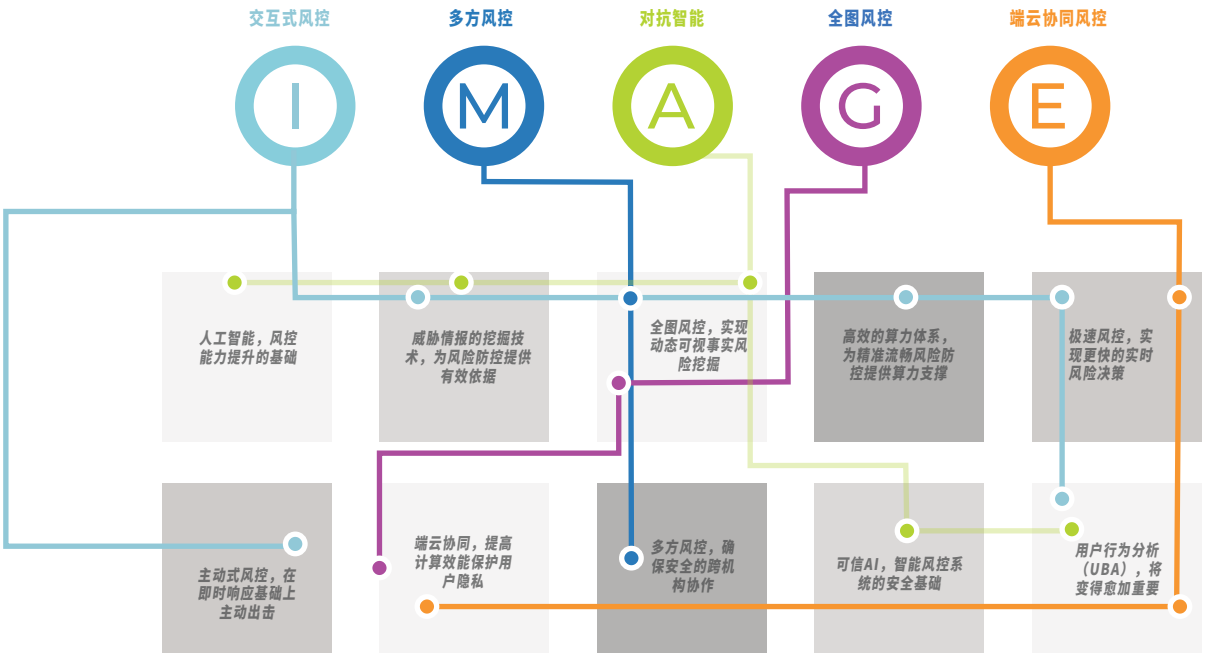
蚂蚁集团解决方案

AlphaRisk风控引擎 —— 基于可信AI的IMAGE风控体系

蚂蚁集团的欺诈管理解决方案多年来服务于支付宝和其生态合作伙伴。TNG Digital表示，蚂蚁集团在欺诈管理领域拥有超过18年的丰富经验，作为TnGD的合作伙伴，蚂蚁集团经常会和TNG Digital分享他们在欺诈管理方面的经验。**AlphaRisk风控**引擎（见图3），融合了上文所提及的新一代反欺诈技术趋势中最关键的能力，合称“IMAGE”，包含交互式风控（Interactivity），多方风控（Multiparty）,对抗智能（Adversarial Learning），全图风控（Graph）和端云协同风控（Edge）。

蚂蚁集团向大中华和亚太地区数字化业务发展最迅速的企业开放的这些新能力，帮助他们在2022年及之后的数字化发展中，始终领先风险一步。

图3 蚂蚁集团AlphaRisk风控引擎：基于可信AI的IMAGE风控体系与2022年欺诈管理领域值得关注的十大能力



来源：IDC金融洞察，2021

图4：蚂蚁集团基于可信AI的IMAGE风控技术体系

关键 技术能力	基础	蚂蚁集团如何利用技术能力来支持其可靠的风险管理系统
 交互式风控	为了让人工智能和机器学习的技术能更可靠的发挥作用，蚂蚁的IMAGE风控体系建立在可信AI框架的基础上，确保了风控系统的安全性、可解释性、公平性和数据安全。	互动式风控将传统的风险防控从以业务为中心转变为以用户为中心。当检测到欺诈风险时，系统不再仅仅拦截交易，而是通过智能交互的方式来提醒用户让其意识到风险，从而自主终止交易。2020年，蚂蚁集团推出了“叫醒热线”，日均成功保护潜在被骗资金2000万，业界均属首次。
 多方风控		为了解决风险防控中的数据孤岛问题，在保护数据安全的情况下实现不同机构间的协作，蚂蚁推出了多方风控平台。它融合了区块链和多项隐私保护的技术，如多方计算（MPC）、可信执行环境（TEE）、联邦学习等等。
 对抗智能		对抗智能建立在博弈论框架之上，通过模拟攻击者和防御者之间的冲突，利用如防御性对抗性权重扰动（AWP）、白盒投影梯度下降（PGD）攻击、卡里尼和瓦格纳（C&W）以及白盒快速梯度标志法（FSGM）等对抗性技术来提高机器学习（ML）模型的鲁棒性。
 全图风控		基于蚂蚁集团自研的工业级图计算平台和大规模图风控基础设施，实现安全风险一张图。可以完成近线分钟级风控动态图算法引擎的部署和流式秒级异常团伙挖掘，让风险防控走在欺诈之前，对团伙及其他批量异常风险要素提前感知。
 端云协同风控		欺诈防控是一场和黑灰产的实时战斗，速率和效率是关键。为了能极速且精准地处理大规模的风险识别，蚂蚁集团推出了端云协同风控的解决方案，既能将用户数据保留在其设备中保护其隐私，也能通过边缘计算更快速、准确地进行风险评估。

来源：蚂蚁集团

重要指导

各企业当前正处在一个十字路口，在数字化趋势带来的积极变革备受鼓舞的同时，也对日益增加的风险保持着警惕。到目前为止，许多企业，包括银行、金融科技公司、支付公司、商户、数字平台供应商等，都在不断思考和讨论战略，研究用户的习惯、偏好和行为的变化，这些变化带来的机会无疑是令人着迷的。

面对新的消费者互动趋势衍生出新的风险，如何从欺诈管理的角度进行应对？这个问题至关重要，一个顺应时代发展的欺诈管理系统是必不可少的。

尽管在数字化程度越来越高、超级交易越来越多、客户渠道越来越广的当今世界，企业有太多机会能够增加收入，然而，仅需一次重大的欺诈事件或者多次小型欺诈案件，所有的收益可能就会付诸东流。

应采取的行动

企业要想始终领先于不断变化的风险，需考虑采取以下行动：

在推出新的产品和服务、新渠道、新的支付方法时，企业需要重新评估现有欺诈防御机制的充分性。之前行之有效的手段，可能在现在这个数字化程度更高的世界里不再可行，因此，欺诈管理能力需要不断升级。本文提出的十大能力为企业提供了新工具、技术和最佳实践的参考。

由于缺乏那些会对系统产生影响的威胁、风险和过往发生的案件认知，企业已深受其害。其实，要做到这一点，或许一套基本的工具也就足够了，但是令人诧异的是，很多机构都缺乏威胁检测的基本工具，甚至是没有对检测到的威胁进行分析的欺诈管理能力。

由于不法分子的攻击手段在不断升级，各机构必须相应地采取针对不同风险的动态策略来进行欺诈检测和预防分析，与时俱进，了解最新的安全解决方案，抛弃那些过时的、不再有效的方案。生物识别认证、新一代认证、用户行为分析、人工智能/机器学习系统等技术正在迅速走向成熟，相信这些新的解决方案会很快在亚太地区的机构中应用开来。

要实现有效的交易和支付欺诈管理，机构须在威胁、成本、可扩展性、效用、数据量、模型效率和客户体验之间不断寻求平衡。一套完备的欺诈管理解决方案能够发挥极大的作用，但是欺诈管理远不仅是建立一套一流的解决方案而已，机构需要多方面考虑其在基础设施、分析能力、人员等方面的投资。

打击欺诈活动需要多方协作，绝不仅仅是建设新的技术能力。反欺诈和运营风险管理项目还应将文化因素考虑在内，符合当地的行为和实践。很多地方政府已经推出了“网络犯罪弹性”计划，帮助大众了解企业在欺诈案件中可能受到的不利影响。此类行动应当继续下去，期望企业能够共同解决欺诈，共同维护数字世界安全。

关于IDC

国际数据公司（IDC）是在信息技术、电信行业和消费科技领域，全球领先的专业的市场调查、咨询服务及会展活动提供商。IDC帮助IT专业人士、业务主管和投资机构制定以事实为基础的技术采购决策和业务发展战略。IDC在全球拥有超过1100名分析师，他们针对110多个国家的技术和行业发展机遇和趋势，提供全球化、区域性和本地化的专业意见。在IDC超过50年的发展历史中，众多企业客户借助IDC的战略分析实现了其关键业务目标。IDC是IDG旗下子公司，IDG 是全球领先的媒体出版，会展服务及研究咨询公司。

IDC China

IDC中国（北京）：中国北京市东城区北三环东路36号环球贸易中心E座901室
邮编：100013
+86.10.5889.1666
Twitter：@IDC idc-community.com
www.idc.com

版权声明