中汇
ZHONGHUI

中国2025第三届跨境数字金融产业合规与共生大会

AI时代跨境业务反欺诈挑战与应对之策

中汇咨询合伙人/ACAMS专家　丘振球

引言：数字金融的新范式

数字技术打破了地域界限，使跨境交易变得前所未有的便捷。然而，这种便利性也为欺诈活动打开了新的大门。 我们面临的不再是零星的、偶发的欺诈案件，而是一场全球性的威胁。

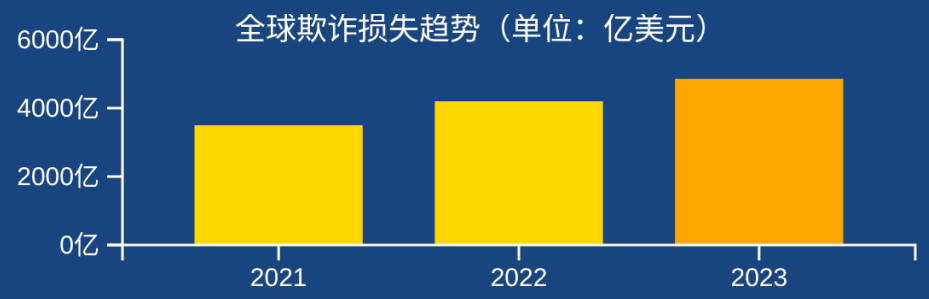
⚠跨境业务的特殊挑战

- 跨境交易涉及多方金融机构、不同司法管辖区和复杂的资金流动
- 交易链条更长，参与方更多，增加了欺诈风险点
- 跨境欺诈往往具有更高的金额和更复杂的结构
- 受害者追回资金的难度通常高于境内交易

全球欺诈损失：触目惊心的数据

2023年全球欺诈损失

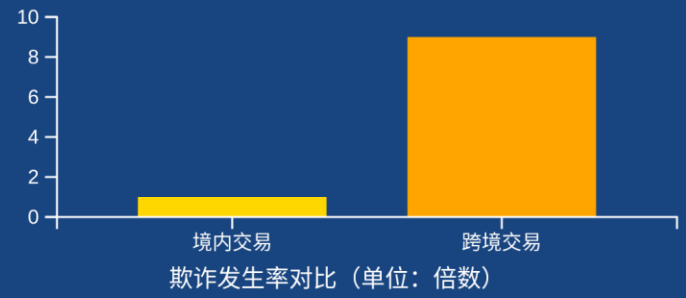
4,856亿美元



跨境与境内欺诈对比

9倍

跨境欺诈发生率是境内交易的9倍



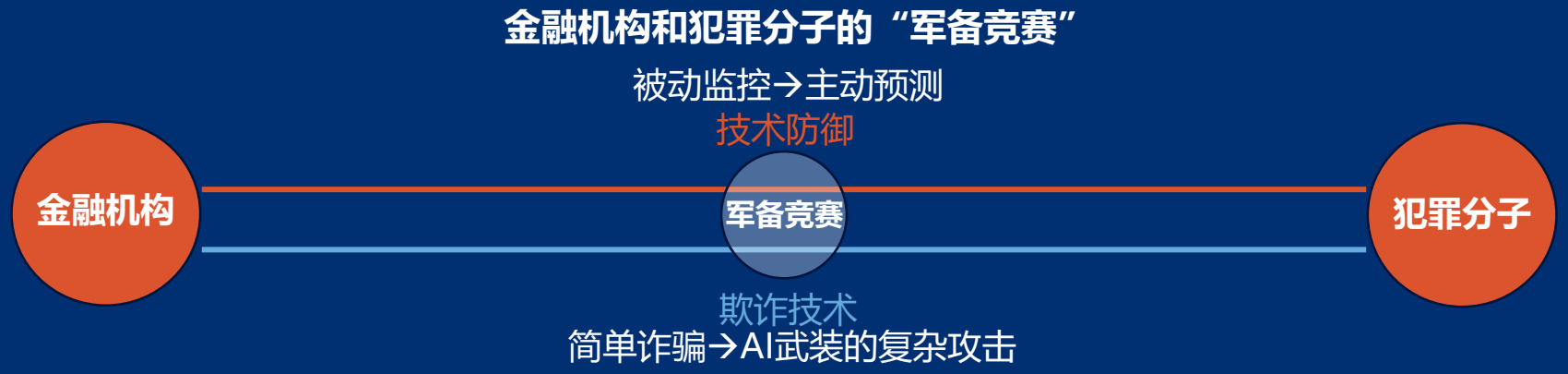
欧洲银行业管理局的分析表明，跨境欺诈的发生率约为境内交易的九倍

行业影响

跨境支付机构面临尤为严峻的形势，作为全球金融体系的连接点，承受着更大的欺诈风险

当前形势："军备竞赛"的开端

我们与金融犯罪分子的斗争，已经演变为一场高科技的"军备竞赛"。一方是利用人工智能武装到牙齿、组织严密、跨国作案的犯罪网络；另一方是肩负合规、风控与客户保护三重使命的金融机构。这场竞赛的胜负，将直接决定全球数字金融生态系统的健康与未来。



欺诈模式的转变

传统"未经授权的欺诈"
破解系统、盗用信用卡等

新型"授权推送支付"欺诈
APP (Authorized Push Payment)

战场的扩展

传统防御目标
保护系统和数据安全

新型防御目标
保护客户认知与判断

挑战：AI成为欺诈者的"超级武器"

人工智能为金融行业带来了效率的飞跃，但当它落入不法分子之手时，便成为了前所未有的"超级武器"。欺诈者利用AI，从四个维度对我们的防线发起了全面攻击。

威胁一：工业化的社会工程学

生成式AI能大规模生成语法完美、措辞地道的超个性化内容，使即便是专业人员也难以分辨真伪。 使得"眼见为实、耳听为虚"的经验法则失效。

威胁二：数字信任的基石侵蚀

深度伪造技术能生成近乎完美的假音视频和伪造生物特征，模仿人的口音、动作和姿态， 足以绕过生物识别认证系统。

威胁三：现有骗局的"超级放大器"

"AI作为"超级放大器"，极大放大了现有跨境骗局的危害。 如"杀猪盘"骗局借助AI聊天机器人同时与上千名受害者建立信任， 导致全球投资欺诈损失激增。

威胁四：犯罪能力的"平民化"

"欺诈即服务"平台的兴起使即便是技术水平不高的个人也能发起复杂攻击。 构建欺诈工具的门槛急剧降低，犯罪成本和技术壁垒被拆除。

威胁一：工业化的社会工程学

生成式AI彻底改变了钓鱼攻击的游戏规则，能够大规模生成语法完美、措辞地道、甚至能模仿特定语气的超个性化内容， 使即便是风险防范意识极强的专业人士也可能落入陷阱。

商业邮件诈骗 (BEC)

犯罪分子通过AI模仿公司高管或长期合作的供应商，发送看似合法的支付指令。

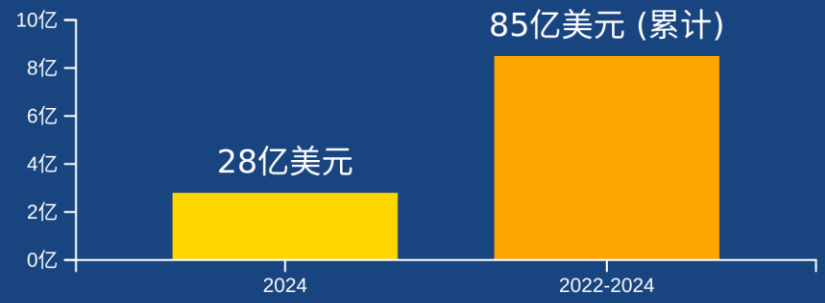
- 身份模仿
- 邮件伪造
- 欺诈指令
- 绕过验证

真实案例

美国中西部地区市政机构案例

- 受害者为资深财务人员，拥有超过5年经验
- 精心伪造的邮件模仿长期供应商
- 未进行电话核实的情况下，批准了欺诈性电汇
- 转账金额高达500万美元

BEC造成的损失



2024年损失
28亿美元

2022-2024年累计损失
85亿美元

检测挑战

传统检测方法难以识别AI生成的内容，因为：

- 语法和逻辑完美，无明显错误
- 高度个性化，针对特定组织
- 难以察觉的微小破绽
- 攻击者有充足时间精心伪造

威胁二：数字信任的基石侵蚀

AI现在能够生成近乎完美的深度伪造（Deepfakes）音视频和伪造生物特征，不仅能模仿人的口音、动作，甚至能模仿其独特的姿态和举止，这足以绕过我们许多核心的生物识别认证系统。

深度伪造的威胁

- 深度伪造技术使"眼见为实、耳听为虚"的经验法则失效
- AI生成的虚假音视频和生物特征足以绕过核心生物识别认证系统
- 香港案例：一名财务人员被深度伪造的视频会议骗走2亿港元

合成身份的崛起

- AI驱动的图像生成技术可创建包含完整数字足迹的"合成身份"
- 虚假身份拥有逼真的证件照片，甚至有关联的社交媒体资料
- 这些身份足以骗过传统的"了解你的客户"（KYC）流程

生物识别系统的脆弱性

- 深度伪造技术能模仿个人独特的口音、动作和姿态
- 即使是最先进的生物识别系统也难以区分真实与伪造
- 攻击者只需获取少量真实数据，即可创建高度逼真的伪造

对金融犯罪风险管理的挑战

- 对反欺诈和反洗钱（AML）框架构成巨大挑战
- 为洗钱活动中至关重要的"钱骡"账户开设提供便利
- 传统验证方法在面对AI生成的虚假身份时几乎无效

"我们长久以来依赖的'眼见为实、耳听为虚'的经验法则，在深度伪造技术面前已经失效。"

案例分析：深度伪造视频会议诈骗

香港一家跨国公司的财务职员接到了一个看似来自公司首席财务官和多位高管的视频会议邀请。在这次会议中， 他按照"上级"的指令，分15次将总计2亿港元的资金转入了多个欺诈账户。

深度伪造视频
AI生成的高管虚假影像

身份伪装
冒充公司高层管理人员

指令诈骗
要求员工进行资金转账

实施诈骗
分15次转入多个欺诈账户

案件发现
警方调查发现全部为AI生成

案件细节

- 受害者：香港跨国公司财务职员
- 诈骗金额：2亿港元（约2560万美元）
- 转账方式：分15次转入多个欺诈账户
- 犯罪手法：利用AI深度伪造技术生成虚假高管形象

关键启示

- 深度伪造技术已从理论走向现实，能够生成足以乱真的视频
- 传统身份验证方式（如"眼见为实"）在数字世界中已失效
- 高级职位人员成为首要目标，因具有更大的决策权和影响力
- 此类攻击不仅针对财务人员，所有涉及决策和资金管理的岗位都面临风险

关键挑战： 我们的战场已经从保护系统和数据，扩展到了保护客户的认知与判断

威胁三：现有骗局的"超级放大器"

除了创造新的攻击手法，AI更像一个"超级增压器"，极大地放大了现有复杂跨境骗局的危害。

"杀猪盘"骗局

一种融合了情感诈骗和投资欺诈的复合型犯罪

- 利用AI聊天机器人同时与成百上千名受害者维持长期情感对话
- AI能不知疲倦地扮演"完美恋人"或"投资专家"角色
- 一旦建立信任，引导受害者至虚假加密货币或外汇投资平台

2023年美国相关损失高达45.7亿美元

威胁四：犯罪能力的"平民化"

过去，发动一场大规模、高技术的跨境欺诈攻击，需要专业的黑客技能、庞大的资源和严密的组织。但现在，AI正在将这种能力"平民化"。

"欺诈即服务"（FaaS）平台

这些平台在暗网上以模块化的方式，向各类犯罪分子兜售"开箱即用"的攻击工具包。

钓鱼网站模板
现成的、可定制的钓鱼页面

恶意软件
窃取支付信息和银行凭证

钱骡网络
用于洗钱的钱骡账户网络

身份盗窃工具
自动化身份信息窃取系统

降低犯罪门槛

- 即便是技术水平不高的个人或小型团伙，也能轻易发起以往只有大型有组织犯罪集团才能实施的复杂攻击
- 利用ChatGPT、v0、n8n等现成的、甚至是免费的AI工具，可在短短几分钟内搭建起高仿品牌网站
- 犯罪的成本和技术壁垒正被AI无情地拆除

战略困境：创新与监管的"不对称性"

欺诈者与金融机构在创新能力上存在根本不对称：欺诈者能不受约束地创新，而金融机构必须在严格监管框架内行事。

欺诈者的优势

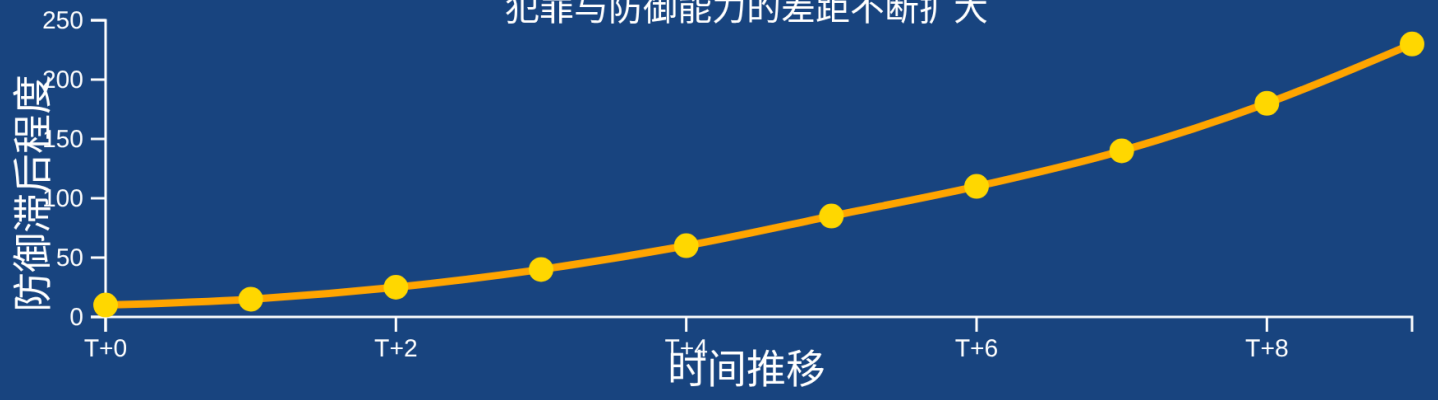
- 利用AI创新，无需受道德、法律或数据隐私约束
- 能够快速迭代，敏捷部署最新攻击战术
- 无需担心合规风险，专注于攻击效果最大化
- 目标单一：寻找监管漏洞和防御薄弱点

金融机构的约束

- 必须在严格的监管框架内行事，受多种法规约束
- 每一次新技术应用都需经过审慎的风险评估和合规审查
- 合规流程复杂，从概念到实施周期长
- 机构间信息壁垒导致防御协同困难

固有不对称导致的结果

犯罪与防御能力的差距不断扩大



突破路径

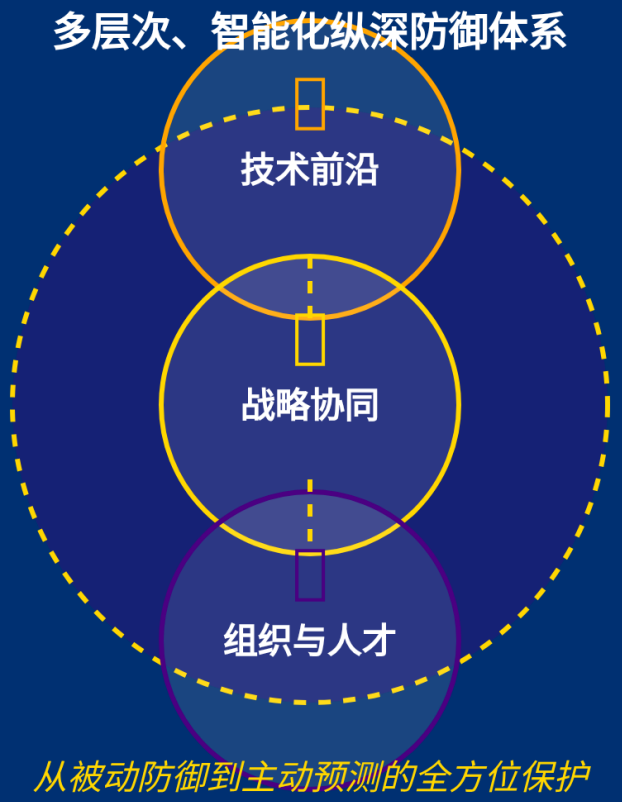
仅依靠增加投入或购买更多传统技术已经无法赢得这场竞赛。

必须寻求根本性战略转变：

- 更高效的情报共享
- 更敏捷的协同作战
- 缩短从威胁出现到有效防御之间的时间差

应对之策：构建多层次防御体系

面对AI武装的对手，我们的防御体系也必须进行智能化、多层次的升级。单点的技术或孤立的部门已无法应对系统性的威胁。 我们必须构建一个集技术前沿、战略协同和人才赋能于一体的纵深防御体系。



1

技术前沿

从被动的基于规则的监控，转向主动的基于预测的防御。利用AI技术构建预测性分析、行为生物识别和可解释AI等核心防线。

2

战略协同

打破内部和外部的信息壁垒，通过公私合作伙伴关系、跨部门数据共享和多机构反诈骗中心，构建协同防御生态。

3

组织与人才

重视专业团队建设和客户教育，通过持续的技能提升和交叉培训，打造人与技术高效协同的综合智能框架。

第一层：技术前沿——以AI对抗AI

对抗自动化、智能化攻击最有效的方式，就是部署同样自动化、智能化的防御系统。我们的思维必须从被动的、基于规则的监控，转向主动的、基于预测的防御。

预测性分析

超越"发生了什么"的描述性分析，迈向预测"可能会发生什么"的预测性分析。通过逻辑回归、决策树和神经网络等机器学习模型，对海量交易和客户行为数据进行深度学习，在欺诈行为造成实际损失前识别高风险账户和交易。

行为生物识别与设备智能

不仅依赖“知道什么”（密码）或“拥有什么”（手机），而是持续地分析“是谁”。通过用户与设备的独特交互方式验证身份，含打字速度与节奏、鼠标移动轨迹、滑动屏幕模式，构成独特的"行为指纹"。

可解释AI (XAI)

解决AI"黑箱"问题，满足监管要求（如欧盟GDPR赋予用户的"解释权"）。XAI技术如SHAP和LIME，能为AI模型的每一个判断提供人类可理解的解释，清晰指出哪些关键特征导致某笔交易被标记为可疑。

主动防御的关键优势

- 从"事后追责"转向"事前预警"，在损失发生前识别并拦截高风险交易
- 利用AI的计算能力，处理和分析传统方法无法处理的海量数据
- 实时调整防御策略，快速适应新型欺诈模式和攻击向量
- 增强模型透明度，提升一线调查人员对AI工具的信任和有效使用

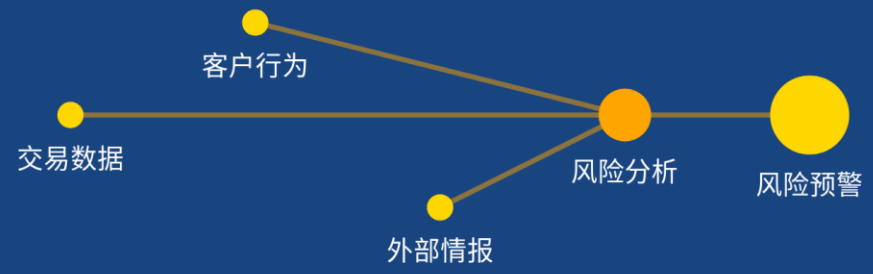
核心技术：预测性分析与行为生物识别

预测性分析

从"发生了什么"的描述性分析，转向"可能会发生什么"的预测性分析

核心技术原理

- 运用逻辑回归、决策树和神经网络等机器学习模型
- 分析海量交易数据、客户行为数据和外部情报
- 在欺诈行为造成实际损失前，精准识别高风险账户和交易

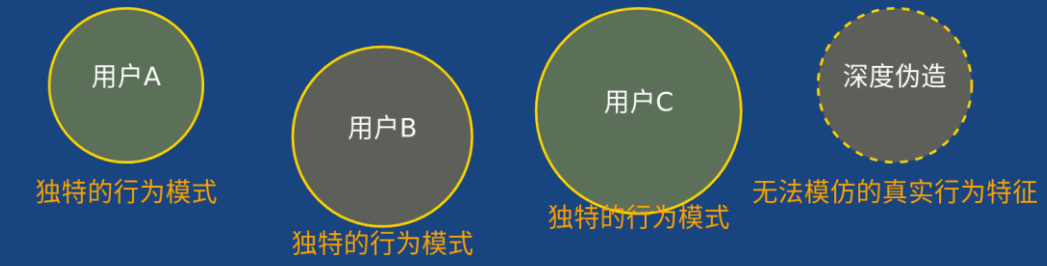


行为生物识别与设备智能

对抗深度伪造和账户盗用的核心防线，分析用户独特的"行为指纹"

行为特征分析维度

- 打字速度与节奏
- 鼠标移动轨迹
- 滑动屏幕模式
- 握持设备角度



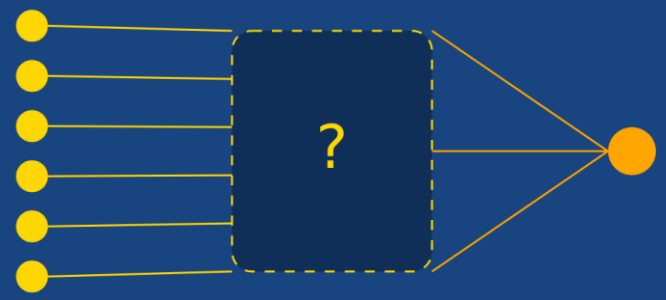
核心优势

- 提前识别风险，防患于未然
- 即使密码被盗，也能验证身份
- 机器无法模仿人类自然行为模式

可解释AI：打破"黑箱"困境

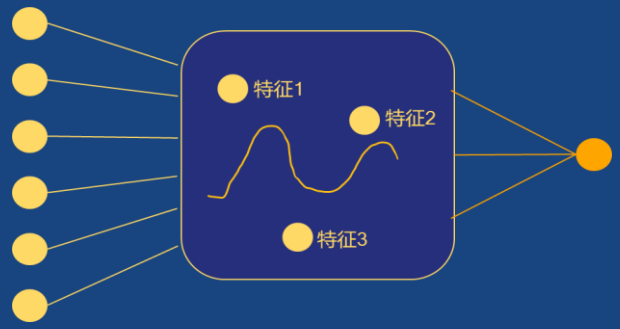
随着防御模型日益复杂，"黑箱"问题日益凸显。可解释AI（XAI）技术为解决这一问题提供了关键方案。

传统"黑箱"AI



难以解释的决策过程，无法追责

可解释AI (XAI)



透明、可追溯的决策过程，提供解释

满足监管要求

符合欧盟GDPR等法规赋予用户的"解释权"，提供模型决策的透明解释

增强模型可信度

使一线调查人员能够信任并有效使用AI工具，提升对可疑交易判断的信心

提升防御效能

减少误报，优化模型，清晰识别关键特征，提高整体防御体系的有效性

XAI技术应用实例

SHAP
提供特征重要性可视化，清晰展示哪些特征导致交易被标记为可疑

LIME
生成局部可解释模型，为AI决策提供人类可理解的逻辑解释

威胁与防御映射矩阵

为了更清晰地展示技术对抗的逻辑，我们可以构建一个威胁与防御的映射矩阵：

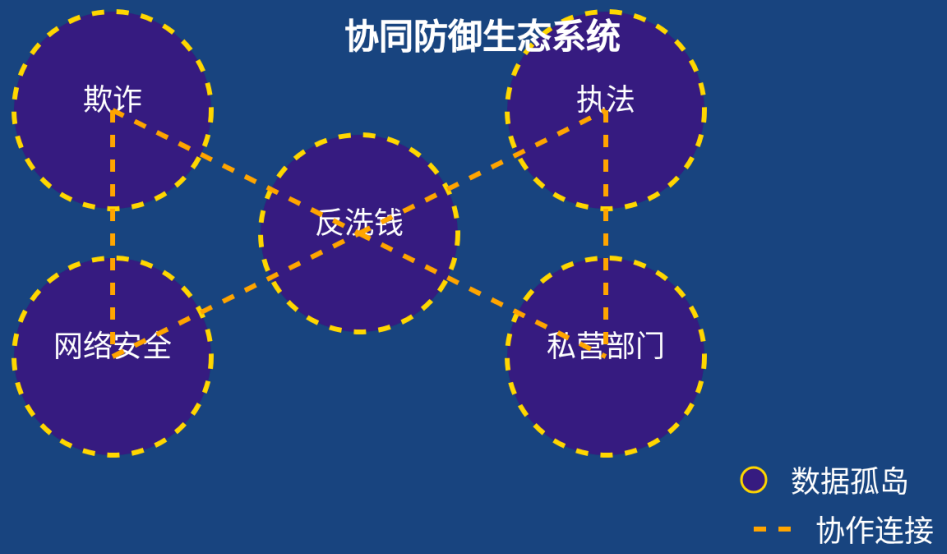
AI驱动的威胁	主要犯罪策略	对应的AI防御机制	核心功能
生成式AI (文本与图像)	超个性化钓鱼、BEC、合成身份文件	**预测性分析、高级异常检测**	在重大损失发生前，识别出通信和交易行为中与既定模式的偏离。
深度伪造 (视频与语音)	绕过生物识别、身份冒充、APP欺诈	**行为生物识别、高级活体检测**	通过分析几乎无法复制的用户独特交互模式（如打字节奏、鼠标移动）进行持续、被动的身份验证。
AI驱动的自动化	大规模凭证填充、机器人攻击、盗卡测试	**设备智能、实时交易监控**	对设备进行指纹识别，并分析地理速度等信号，在毫秒间区分合法人类用户与自动化脚本。
AI模型学习 (对抗性)	规避静态、基于规则的系统	**可解释AI、自适应机器学习**	增强模型透明度以便快速优化，并使防御模型能够实时从新的欺诈类型中学习和适应。

关键洞察：以AI对抗AI 已成为现代金融安全的必然趋势

第二层：战略协同——打破藩篱

技术是必要条件，但绝非充分条件。在这场全球性的对抗中，没有任何一家机构能够单打独斗取得胜利。各自为战的"数据孤岛"和情报壁垒，是犯罪网络最乐于利用的漏洞。胜利要求我们从根本上转向一个协同防御的生态系统。

从"数据孤岛"到"协作生态"的转变



战略转变

我们需要从"各自为战"的旧思维，转向"敢于共享"的新理念，打破内部与外部的信息壁垒。

内部壁垒

打破欺诈、网络安全和反洗钱团队之间的内部壁垒，整合不同职能部门的情报和资源。

外部壁垒

摒弃私营部门与执法机构之间的外部壁垒，建立互信机制，共享战略层面的欺诈类型、犯罪网络和资金流向情报。

风险预防：公私合作与跨部门数据共享

在全球性金融犯罪面前，任何机构单打独斗都难以取得胜利。打破内部与外部壁垒，构建协同防御生态系统成为当务之急。

公私合作伙伴关系 (PPPs)

打破欺诈、网络安全和反洗钱团队之间的内部壁垒，以及私营部门与执法机构之间的外部壁垒。

英国JMLIT

联合欺诈调查团队，整合执法与金融行业资源，提升打击金融犯罪的协同效能。

美国FinCEN Exchange

金融犯罪执法网络交换平台，促进联邦机构间的战略情报共享，优化资源配置。

跨部门数据共享平台

立法和监管创新是实现高效协同的关键。新加坡的COSMIC平台通过"敢于共享"（dare-to-share）理念，开创了跨部门数据共享的新范式。

新加坡COSMIC平台

全称：跨组织市场信息和跨境犯罪共享平台（Cross-Organisation Sharing of Market Information and Cross-border Crime）

- 通过立法授权，允许金融机构在保护客户隐私的前提下，安全、实时地共享与重大金融犯罪风险相关的客户信息
- 实现了"敢于共享"（dare-to-share）的数据协作模式

成功合作的关键效益

- 建立互信机制，共享战略层面的欺诈类型、犯罪网络和资金流向情报
- 突破信息孤岛，实现机构间的战略协作与情报融合
- "敢于共享"（dare-to-share）的理念代表了未来协同反欺诈的方向

执法止损：多机构反诈骗中心模式

在亚太地区，包括新加坡、澳大利亚、香港等地，已经涌现出由执法部门、金融机构、电信运营商和科技公司共同组成的多机构反诈骗中心(ASCs)。这些中心实现了情报的融合与行动的统一，能够在欺诈交易发生的初期就进行实时干预。

多机构反诈骗中心构成

执法机构
提供法律授权和执法支持，处理欺诈调查和起诉

金融机构
提供金融交易监控和资金冻结能力，识别可疑交易

电信运营商
提供通信网络监控和拦截服务，阻断诈骗通信

科技公司
提供网络安全和AI技术支持，增强防御能力

协同作战优势

实时干预
在欺诈交易初期就进行资金冻结和通信阻断

情报融合
整合多源情报，识别复杂的欺诈模式和网络

行动统一
实现跨机构协作，避免信息孤岛和重复工作

资源优化
集中资源和专业知识，提高整体防御效能

第三层：组织与人才——决胜于人

归根结底，我们最强大的防御武器，以及最脆弱的环节，都是人。技术赋予我们能力，但最终的决策、判断和创新，依然源于专业的团队和具备风险意识的客户。

专业技能升级与认证

- 对欺诈、反洗钱和网络安全团队进行持续的技能提升和交叉培训
- ACAMS的"注册反欺诈师"(CAFS)认证，系统性地涵盖欺诈风险管理、检测与分析、调查以及反欺诈技术等核心知识领域
- 培养面向未来的复合型专家，为行业输送专业人才

专业认证的价值：

提供系统化、国际认可的专业标准，确保团队具备应对新型欺诈威胁的专业能力

客户教育的升级

- 传统的静态风险提示邮件或弹窗，面对超个性化骗局效果有限
- 未来的客户教育必须是动态的、嵌入式的、与场景紧密结合的
- 利用技术，在客户交易旅程中，通过"行为干预"方式进行实时提醒

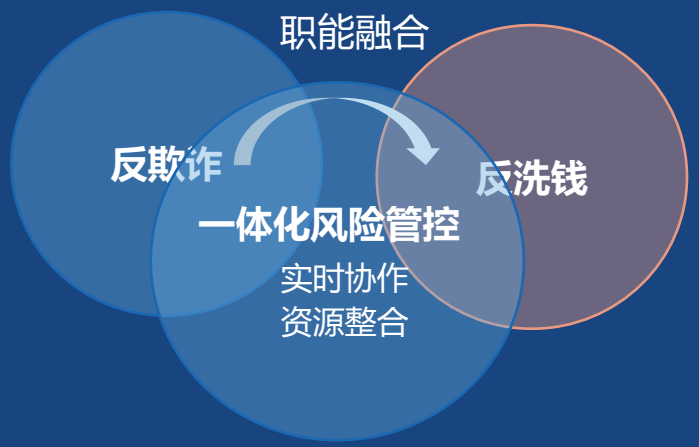
创新案例：

当系统发现老年客户进行大额、高风险转账，且行为特征与被远程操控的特征吻合时，自动触发强制冷静期或交互式问答，唤醒客户风险意识

反欺诈与反洗钱的融合趋势

长期以来，反欺诈与反洗钱在很多机构内是独立运作的职能部门。然而，今天的现实是，两者之间的界限已经变得模糊，甚至在很多场景下已经消失。未来金融犯罪风险管理的必然走向是一体化模式。

反欺诈与反洗钱融合的必要性



融合的关键驱动力

- 欺诈所得已成为洗钱活动最主要的上游犯罪收益来源
- 合成身份的主要目的是用于开设钱骡账户，作为洗钱网络的初始节点
- 欺诈行为的完成，往往就是洗钱行为的开始
- 维持部门墙将导致情报割裂、响应迟缓和资源浪费

全链路可视性

整合欺诈识别、AML监控和网络安全防御，实现对风险的完整视图

实时协同响应

统一指挥和分析平台，实现多维度情报共享，缩短从威胁到防御的时间差

资源优化配置

消除职能重复和资源浪费，集中专业力量应对复合型金融犯罪

> **“未来的金融犯罪风险管理，必然走向一个一体化的模式”**

中汇 ZHONGHUI

感谢您的观看

Thank You For Watching

联系邮箱：qiuzq@zhcon.cn

微信号： Michael18212455

联系电话：18665653639