# 针对合成身份欺诈、身份盗用、账户接管的关键防线

## 不断演变的威胁格局

### 客户开户：身份盗用和合成身份欺诈

- 身份盗用利用窃取的真实个人识别信息 (PII) 和文件来冒充真实个人。
- 合成身份欺诈故意混合真实和伪造的属性，通过合理且一致的身份数据创建可扩展的虚构身份。
- 合成身份通常能顺利通过开户检查，因为欺诈分子会从头到尾伪造身份、历史记录和文件。
- 由于合成身份欺诈并无明确的受害者，会导致延迟报告的问题，令欺诈分子有时间逐渐建立信任。

### 开户后：账户接管 (ATO) 欺诈

- 攻击者通过网络钓鱼诈骗、SIM 卡交换、中间人技术窃取凭证。
- 单独使用一次性密码 (OTP) 和静态身份验证因素越来越无效。
- 人工智能 (AI) 可跨渠道实现自动化、规模化和持久性。

### 人工智能支持的假冒（跨生命周期）

- 深度伪造令攻击者能大规模创建合成身份，然后当成武器进行欺诈。
- 人脸交换、语音克隆、注入攻击能绕过不全面的活体检测和在线身份验证系统。
- 威胁行为者越来越多地同时利用人工智能生成的媒体、被攻击的设备和模拟行为，规避管控措施。

**传统验证为何会失败**

- 文件和个人身份信息不再是可靠的真相锚点：
    - 被盗的身份以合法文件和数据作为后盾
    - 欺诈分子生成或获取高度令人信服的文件，支持其伪造身份。
- 时间点检查无法监测跨会话或跨渠道的异常情况。
- 基于 OTP 的控制措施在 SIM 卡交换、恶意软件和重放攻击面前毫无还手之力。
- 传统验证无法监测 AI 辅助注入或实时假冒。

## 持续验证个人身份

- 通过执行实时多信号一致性来增加攻击者成本。
- 通过专用模型进行风险评分，从而区分合成身份欺诈、身份盗用、账户接管。
- 在整个客户生命周期中，从静态验证过渡到基于风险的自适应身份验证。

## 威胁矩阵：监测和减少新兴身份欺诈

| 欺诈威胁 | 关键信号 | 监测方式 | 减少方式 |
|---|---|---|---|
| 合成身份欺诈 | 一致但人造的个人身份信息、最少的文件历史记录、身份重用模式 | 人工智能协助文件核查、设备/身份绘图、联合信号 | 网络分析、跨机构关联、基于风险的开户 |
| 身份盗用 | 行为或设备不一致的合法文件 | 生物识别和活体检测、设备智能、行为不匹配 | 逐步身份验证、生物识别重新验证、持续监控 |
| 账户接管 | 行为变化、新设备/IP、会话异常 | 行为生物识别、会话风险评分 | 自适应逐步控制、实时干预、交易层面核查 |

## 设计原则 & 最佳实践

- **风险偏离：**在开户过程中，而不是*在损失*发生后才对深度伪造和注入企图进行监测。
- **默认为自适应：**根据行为、设备和背景，动态上报控制措施。
- **持续确保：**针对高风险活动，基于行为生物识别技术持续对用户身份进行重新验证。
- **可解释的决定：**支持调查，协助完成监管审查。
- **共享情报：**利用联盟和威胁情报源，揭示新出现的攻击手段、技术和程序 (TTP)。
- **韧性测试：**针对基于 AI 的攻击，定期开展红队控制操作。

## 呼吁行动

- 假设身份可以伪造得令人信服，相应地设计控制措施。
- 不再将文档和 OTP 看做基本信任信号。
- 对人工制品、行为、设备和网络信号进行分层监测
- 针对不断演变的深度伪造工具，持续测试防御措施。

**进一步阅读**

- FBI IC3 PSA: Synthetic Identity Fraud;
- DHS / HSI Intelligence Bulletin on Fraud Networks;
- Unmasking Cybercrime: Strengthening Digital Identity Verification against Deepfakes