Líneas de defensa clave contra el fraude de identidad sintética, el robo de identidad y la toma de control de cuentas

El panorama de amenazas en evolución

Onboarding de clientes: robo de identidad y fraude de identidad sintética

- El robo de identidad aprovecha la información personal identificable (PII, por sus siglas en inglés) y los documentos auténticos robados para suplantar la identidad de personas reales.
- El fraude de identidad sintética combina deliberadamente atributos reales y ficticios para crear identidades escalables y ficticias con datos de identidad plausibles y coherentes.
- Las identidades sintéticas suelen superar los controles de onboarding porque el estafador crea la identidad, el historial y la documentación de principio a fin.
- La ausencia de una víctima clara en el fraude de identidad sintética retrasa la denuncia y permite a los estafadores establecer gradualmente su credibilidad.

Después de la apertura de la cuenta: toma de control de cuentas (ATO, por sus siglas en inglés)

- Los atacantes comprometen las credenciales mediante estafas de phishing, intercambios de SIM y ataques de intermediario.
- Las contraseñas de un solo uso (OTP, por sus siglas en inglés) y los factores de autenticación estáticos son cada vez menos eficaces cuando se utilizan por sí solos.
- La inteligencia artificial (IA) permite la automatización, la escalabilidad y la persistencia en todos los canales.

Suplantación de identidad habilitada por IA (a lo largo de todo el ciclo de vida)

- Los deepfakes permiten a los atacantes crear identidades sintéticas a gran escala y utilizarlas como arma para cometer fraudes.
- Los intercambios de rostros, la clonación de voces y los ataques de inyección pueden eludir los controles de autenticidad inadecuados y los sistemas de verificación de identidad en línea.
- Los actores de amenazas combinan cada vez más medios generados por IA, dispositivos comprometidos y emulación de comportamiento para evadir los controles.

Por qué falla la verificación tradicional

- Los documentos y la PII ya no son fuentes confiables de información:
  - Las identidades robadas están respaldadas por documentos y datos legítimos.
  - Los estafadores pueden crear u obtener documentos muy convincentes para respaldar identidades sintéticas.
- Las comprobaciones puntuales no pueden detectar anomalías entre sesiones o entre canales.
- Los controles basados en OTP son vulnerables a los intercambios de SIM, el malware y los ataques de retransmisión.
- La verificación tradicional no fue diseñada para detectar inyecciones asistidas por IA o suplantaciones de identidad en tiempo real.

Autenticar continuamente a la persona

- Aumenta los costos para los atacantes aplicando la coherencia multiseñal en tiempo real.
- Puntuación de riesgo y distinción entre fraude de identidad sintética, robo de identidad y ATO con modelos específicos.
- Transición de la verificación estática a la autenticación adaptativa basada en el riesgo a lo largo del ciclo de vida del cliente.

Matriz de amenazas: Detección y mitigación de nuevas modalidades de fraude de identidad

Amenaza de fraude	Señales clave	Cómo detectar	Cómo mitigar
Fraude de identidad sintética	PII coherente pero artificial, historial mínimo de archivos, patrones de reutilización de identidades	Verificación de documentos asistida por IA, gráficos de dispositivos/identidades, señales de consorcio	Análisis de redes, vínculos entre instituciones, onboarding basado en el riesgo
Robo de identidad	Documentos legítimos con inconsistencias de comportamiento o del dispositivo	Verificaciones biométricas y pruebas de vida, inteligencia de dispositivos, discrepancias de comportamiento	Autenticación reforzada, reverificación biométrica, supervisión continua
Toma de control de cuentas	Cambio de comportamiento, nuevo dispositivo/IP, anomalías en la sesión	Biometría conductual, puntuación de riesgo de sesión	Controles adaptativos de escalada, intervención en tiempo real, comprobaciones a nivel de transacción

Principios de diseño y prácticas recomendadas

- **Anticipar la gestión del riesgo:** detecte intentos de deepfake e inyección durante el onboarding, no *después* de las pérdidas.
- **Adaptable por defecto:** escale los controles de forma dinámica en función del comportamiento, el dispositivo y el contexto.
- **Aseguramiento continuo:** vuelva a autenticar continuamente a los usuarios basándose en biometría conductual durante actividades de alto riesgo.
- **Decisiones explicables:** apoye las investigaciones y ayude a abordar el escrutinio regulatorio.
- **Inteligencia compartida:** utilice fuentes de información sobre consorcios y amenazas para detectar tácticas, técnicas y procedimientos (TTP) de ataque emergentes.
- **Pruebas de resiliencia:** realice periódicamente operaciones de control del equipo rojo contra ataques habilitados por IA.

Llamado a la acción

- Suponga que la identidad puede falsificarse de manera convincente; diseñe los controles en consecuencia.
- Vaya más allá de los documentos y las contraseñas de un solo uso como señales fundamentales de confianza.
- Detección de capas en artefactos, comportamiento, dispositivos y señales de red.
- Pruebe continuamente las defensas contra las herramientas deepfake en constante evolución.

Lectura adicional

- **Aviso público del FBI IC3: Fraude de identidad sintética;**
- **Boletín de inteligencia del DHS/HSI sobre redes de fraude;**
- **Desenmascarar los ciberdelitos: fortalecimiento de la verificación de identidad digital contra los deepfakes**