PUERTO RICO FINANCIAL SERVICES FORUM

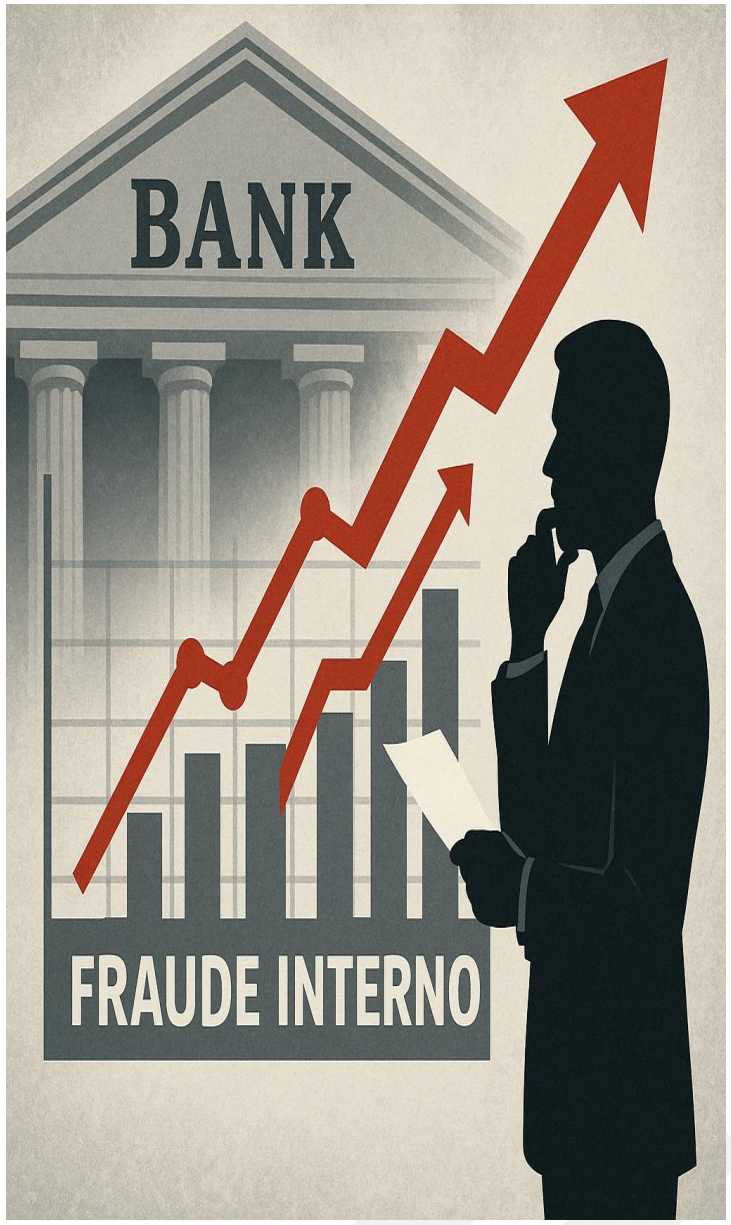
Alejandro Mijares
Fundador/CEO
Mijares Consulting
11.17.2025

“CYBER RISK: TRANSFORMING THE LANDSCAPE OF FRAUD”

(RIESGO CIBERNÉTICO: TRANSFORMANDO EL PANORAMA DEL FRAUDE)

- Tendencias Regulatorias en USA en el 2025
- Casos de fraude en Bancos en USA
- Casos de fraude en Bancos en Miami
- Controles
- Que dice ChatGPT de la IA y fraude?

Tendencias Regulatorias en USA en el 2025



- El riesgo operativo se mantiene alto

- Tendencia creciente de actividad de fraude externo explotando métodos de pagos tradicionales:
  - Cheques (dark web, alteración de beneficiarios, firmas y cheques falsificados)
  - Transferencias electrónicas
  - plataformas de pagos entre pares (P2P)
  - Empleados internos

- Riesgo de Ciberseguridad:
  - Proveedores (punto único de falla)
  - Ransomware (ataques de doble extorsión)
  - Cajeros Automaticos (Jackpotting y vaciado)
  - Ingeniería social
  - Phishing
  - Toma de control de cuentas
  - Compromiso de correo electrónico empresarial y suplantación de identidad

Casos de fraude en Bancos en USA
Análisis de sansiones en el 2025

- Menos órdenes a instituciones, más prohibiciones a personas.
- El fraude se “mueve” a donde hay supervisión débil: sucursal, ATM, imágenes, canales digitales.
- La Junta es responsable de exigir programas de seguridad de la información basados en riesgo.
- Fraude Interno:
  - Venta/filtración de imágenes de cheques desde sistemas internos
  - Acceso indebido a información de clientes y uso para fraude
  - Sustracción en ATM con ajuste de totales para “cuadrar” balances

“En 2025, la OCC dejó algo claro: si los controles fallan, las personas pagan…y la Junta responde.”

“No basta con tener políticas; la evidencia de funcionamiento es el nuevo estándar.”

Casos de fraude en Bancos en Miami

PHISHING

ACCOUNT TAKEOVER

VIRTUAL FRAUDULENT ACCOUNTS

Controles

- Capacitación a empleados
- Monitoreo de comportamiento atípico
- Pruebas de penetración
- Reforzar los controles y el monitoreo para gestionar el riesgo de fraude de manera efectiva
- Apoyo a clientes mediante educación sobre ciberseguridad, tendencias emergentes de fraude. y medidas de protección
- Controles internos adecuados, como la autenticación, los procesos de identificación y verificación del cliente, y el monitoreo de fraude
- DLP (contenido/etiquetado)
- Logs y respaldos inmutables
- Ejercicios de Table-top de exfiltración e data (Respuesta a Incidentes)

ChatGPT 5.1

PUERTO RICO
FINANCIAL SERVICES
FORUM

Cómo la IA puede ser utilizada para facilitar fraudes en bancos

- Deepfakes avanzados
- Ingeniería social automatizada
- Manipulación y falsificación de documentos
- Automatización del fraude con datos sintéticos
- Elusión de autenticaciones biométricas
- Explotación de modelos de IA del banco

Líneas estratégicas de respuesta para instituciones financieras

- Autenticación avanzada y análisis de comportamiento
- Detección de deepfakes y validación reforzada de identidad
- Modernización del programa de fraude con IA defensiva
- Gobernanza fortalecida del uso de IA y gestión de modelos
- Mayor rigor en gestión de terceros (TPRM)
- Educación continua a empleados y clientes sobre nuevas amenazas

PUERTO RICO
FINANCIAL SERVICES
FORUM

www.mijares.consulting

www.linkedin.com/compan
/mijaresconsulting/

www.youtube.com/@Mijar
sConsulting