



Estrategia y Mejores Prácticas para Proteger los Medios de Pago

Maribel Corrales

Directora de Riesgo Latinoamérica y Caribe





Permitir pagos rápidos, convenientes y seguros mediante la protección, el aprovechamiento y la devaluación de los datos y el empoderamiento de los consumidores.

Maribel Corrales

Directora de Riesgo Latinoamérica y Caribe



Aviso Legal

Resultados de encuestas, investigaciones y recomendaciones de mejores prácticas se proporcionan “COMO ESTÁ”, solamente para fines informativos y no deberán ser consideradas como asesoría comercial, legal, regulatoria, fiscal, financiera o de otro tipo. Recomendaciones de mejores prácticas o materiales deben evaluarse por separado en base a sus propias necesidades comerciales específicas y en vista de las leyes y normativas que aplican a su situación particular. Visa no es responsable por el uso que usted pueda hacer de los resultados de encuestas, investigaciones o recomendaciones de mejores prácticas ni de ninguna otra información, incluidos errores de cualquier tipo, ni por cualquier presunción o conclusión que usted pudiera inferir del uso de los mismos.

Esta presentación podría contener declaraciones a futuro según se definen en la ley de Estados Unidos conocida como el Private Securities Litigation Reform Act de 1995. Estas declaraciones se pueden identificar por los términos “esperar”, “será”, “continuar” y referencias similares al futuro. Por su naturaleza, las declaraciones a futuro: (i) se refieren únicamente a la fecha en que son realizadas; (ii) no son declaraciones de hechos históricos ni garantía sobre desempeño futuro; y (iii) se encuentran sujetas a riesgos, incertidumbre, suposiciones y cambio de circunstancias que difícilmente se pueden predecir o cuantificar. Visa describe en sus notificaciones registradas con la SEC los riesgos e incertidumbres que pudieran dar lugar a que los resultados finales difieran de manera importante o se opongan a declaraciones a futuro. A menos que la ley lo requiera, Visa no tiene intención de actualizar o revisar cualquier declaraciones a futuro aquí contenida en virtud de nueva información, eventos futuros o por cualquier otra razón.

Agenda



1



Amenazas de Fraude en los Medios de Pagos

2



Principales Tendencias de Seguridad

3



Recomendaciones

Amenazas de Fraude en los Medios de Pago

Las tecnologías emergentes presentan un futuro incierto

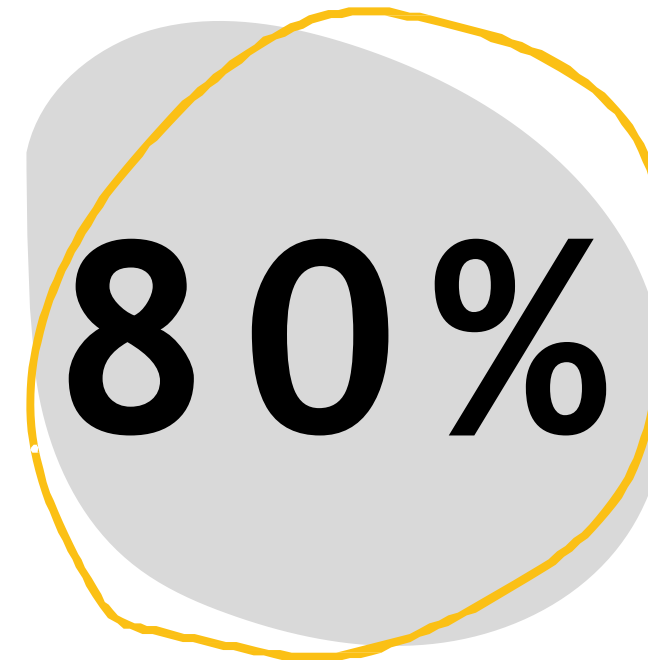
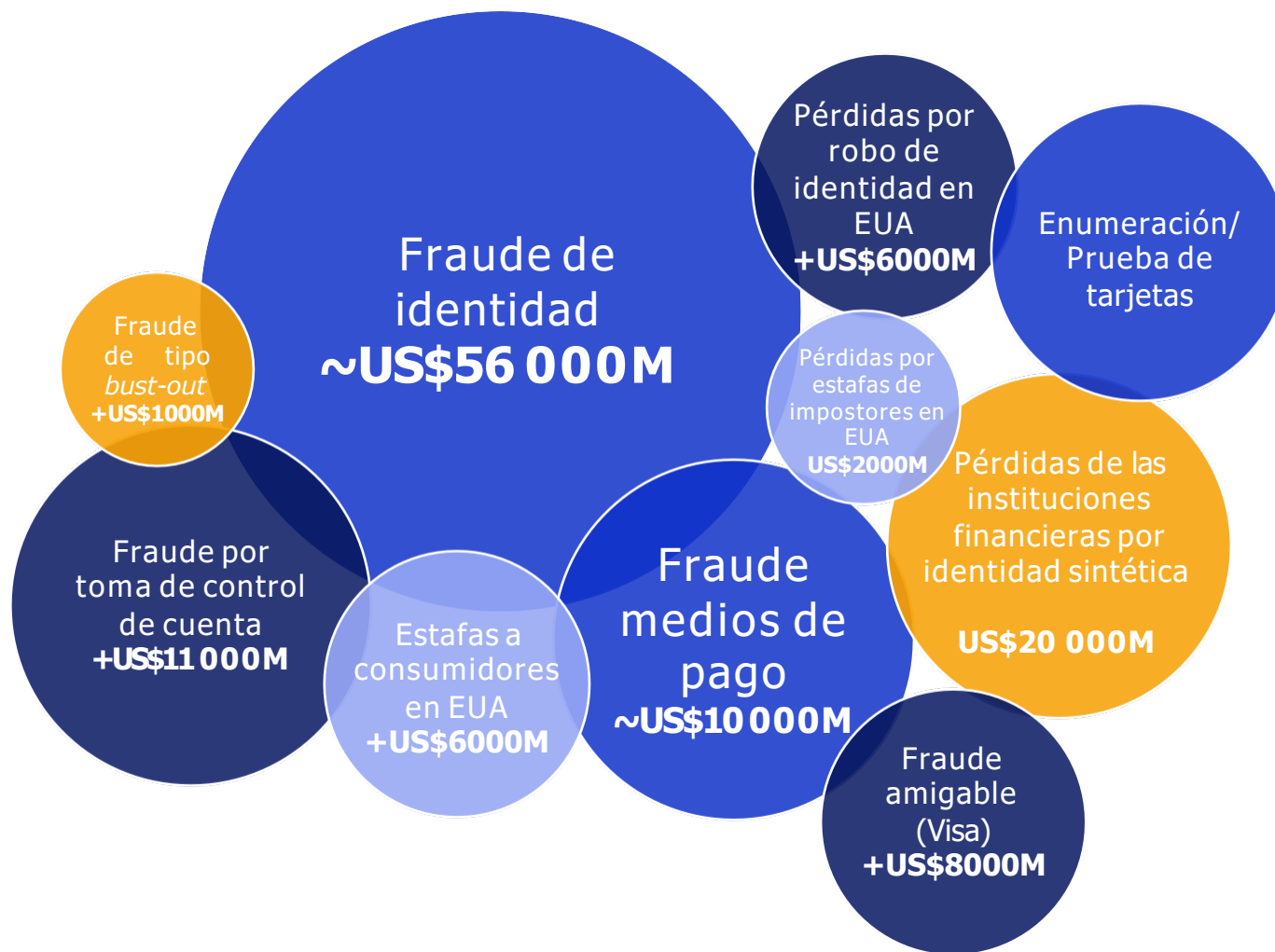


**En medio del caos,
también hay
oportunidades.**

Sun Tzu



El fraude congestiona y contamina nuestro ecosistema



De las contraseñas son la causa raíz de los compromisos de información (*data breaches*).

Fuentes: <https://www.experian.com/blogs/ask-experian/identity-theft-statistics/>, <https://www.idx.us/knowledge-center/the-real-cost-of-identity-theft-to-employees-businesses>, <https://www.veriff.com/blog/account-takeover-fraud-statistics>, <https://chargebacks911.com/bust-out-fraud/>, <https://www.pymnts.com/news/banking/2022/p2p-payments-fraud-suggests-liability-gray-area/>, <https://www.pymnts.com/identity-theft/2022/synthetic-identity-fraud-costs-businesses-billions-each-year-data-shows/>. Índice obtenido con US\$10B x .5% para disputas x 17% para fraude amigable.
*fidoalliance.org.

Las amenazas de fraude en los medios de pagos se han vuelto muy sofisticadas y plantean un riesgo significativo..

Panorama de ataques en evolución

En el pasado...

... Los malos actores se especializaban predominantemente en sus propias áreas de especialización y eran grupos poco organizados dirigidos a individuos.

En el entorno actual...

... Los delincuentes son redes de actores de amenazas altamente calificados y con buenos recursos que apuntan a los activos tecnológicos de corporaciones más grandes y su infraestructura interconectada.

Amenazas primarias



Ataques de enumeración

40 millones de transacciones enumeradas al mes a nivel mundial¹



Secuestro de datos - Ransomware

20 mil millones de dólares anuales en daños a nivel mundial para 2022



Skimming and Malware

4X aumento en CNP comprometidos debido a skimming³



Ingeniería social

19% incremento en account takeover-relacionado con fraude⁵



Los Delitos Financieros son cada vez más Sofisticados

El fraude tradicional con tarjetas Visa es la punta del iceberg



\$20^{*}B

Pérdidas anuales estimadas por fraude de identidad sintética

68% *



Aumento anual de compromisos de datos



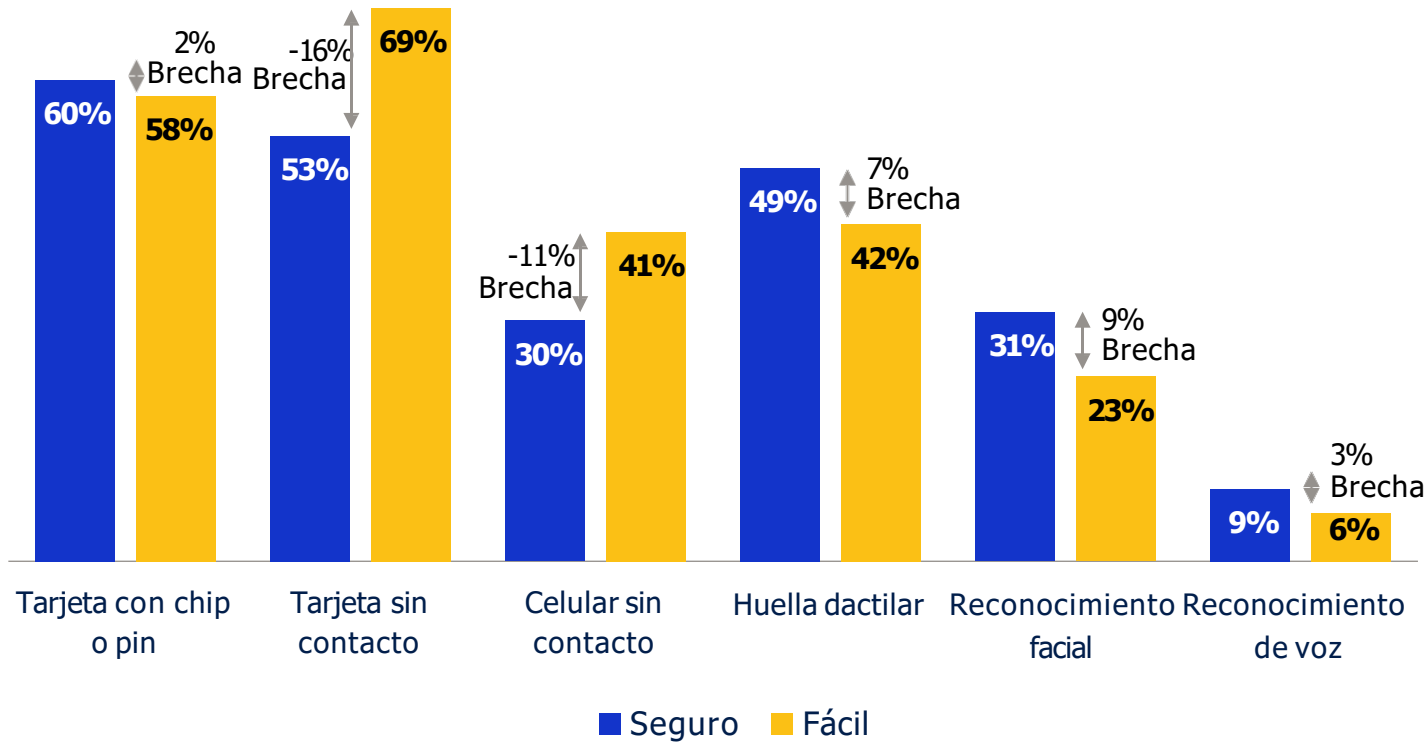
*Study via Federal Reserve of Boston in 2020 with references to Identity Theft Resource Center's 2021 Annual Report – links below
<https://www.bostonfed.org/news-and-events/news/2022/08/synthetic-identity-fraud-is-not-a-victimless-crime-costs-billions-damages-lives.aspx>
<https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/>

Los Tarjetahabientes buscan Confianza, Seguridad y Comodidad



Resultados de encuestas en el mercado de América Latina

Percepciones de cuáles métodos de pago son más seguros y cuáles facilitan la vida



Métodos de autenticación cuando se usa una nueva cuenta o app

"inicio sesión con mi..."



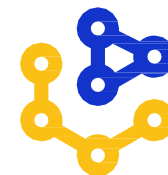


En general se ha estado utilizando **inteligencia artificial** para **proteger los pagos** durante décadas, pero la tecnología está proliferando rápidamente entre los estafadores.

VISA



Mayor sofisticación de la suplantación biométrica



Ingeniería social aprovechando las herramientas de IA generativa



Carrera de armas impulsada por inteligencia artificial entre atacantes y defensores

Las 5 principales tendencias para la seguridad de los pagos

Las 5 principales tendencias para la seguridad de los pagos

La inteligencia artificial aumenta la sofisticación de la ingeniería social

Barreras reducidas para cometer fraude

Clientes esperan procesos de pago más fluidos

Las innovaciones de pagos emergentes se enfrentan a vientos en contra

Los estafadores se sienten atraídos por las primeras etapas del ciclo de vida de las transacciones



EMERGING INNOVATIONS FACE HEADWINDS

Los estafadores se mudan a rieles de pago menos maduros



Pagos con tarjeta

Visa ayuda a detener \$ 26 mil millones de fraude anualmente con herramientas de riesgo del emisor que reducen nuestra superficie de ataque

Pagos en tiempo real

El aumento de la ingeniería social brinda a los estafadores acceso a fondos reales en tiempo real con menos protección para el consumidor a medida que crece la superficie de ataque

Crypto Blockchain

Aún no se ha determinado cómo afectará la regulación a las criptomonedas y cómo se realizan los pagos en la cadena de bloques.

Tipos de pagos futuros

Recomendaciones

VISA INVESTMENTS IN SECURITY

Invertir en tecnología e innovación durante los últimos años, ha logrado el resultado de detener a los estafadores y proteger a los comercios y consumidores de las pérdidas por fraude



SECURING THE ECOSYSTEM

Proteger

Contra potenciales
amenazas

Defender

contra los ataques
en curso



Adaptar

gestión de riesgos a
sus necesidades
únicas

Evolucionar

capacidades con el
landscape cambiante

La inversión es clave para la mitigación de riesgos

- 1 Monitoreo en tiempo real
- 2 Verificación de identidad
- 3 Educación / Capacitación
- 4 Actualización de software
- 5 Cumplir con las regulaciones



¡GRACIAS!