La seguridad en los medios de pago: una responsabilidad compartida

Comisión de Economía del Senado

Valparaíso, Chile

2 de agosto de 2017

Objetivos de la presentación

1. Explicar la evolución reciente en medios de pago y sus implicaciones para la seguridad

2. Compartir nuestra visión de la seguridad como una responsabilidad compartida de todos los participantes en la cadena pagos

3. Compartir consideraciones finales sobre el proyecto de modificación a la Ley 20.009

El ambiente de compras está cambiando

Cara a cara

Por Internet

Hacer clic y recoger

Híbrido

La distinción entre pagos en el mundo físico y el digital se está borrando cada vez más rápidamente

El POS está en todos lados...

Nota: Los nombres y logos de marca son propiedad de terceros y son usados a titulo ilustrativo solamente, sin suponer validación de productos o afiliación con Visa

Las transacciones digitales son el vehículo del crecimiento en consumo y reto para el comercio

	POS físico	Comercio electrónico	Móvil
			
Crecimiento*	4%	11%	38%

Fuente: eMarketer estimados 2014-2015

El rol de Visa

- Generar **confianza y conveniencia** al realizar pagos electrónicos
- Maximizar la **seguridad de los pagos electrónicos** independientemente del dispositivo o canal
- Ampliar inclusión financiera mediante mayor **acceso y uso de pagos electrónicos** entre consumidores y comercios

Seguridad en pagos: responsabilidad compartida

Múltiples actores en la cadena de pagos

Adquirente
Institución que afilia y vincula a los comercios al sistema Visa, les procesa transacciones y les realiza liquidaciones financieras.

Visa
Red de Pagos, facilita la transferencia global electrónica de fondos a través de productos de pago.

Emisor
Institución que emite tarjetas y mantiene una relación financiera con el Tarjetahabiente.

Procesador Adquirente
Realiza servicios de procesamiento para los Adquirentes.

Procesador Emisor
Realiza servicios de procesamiento para los Emisores.

Proveedor de Servicios para Procesamiento de Pagos
Provee servicios de valor agregado y conectividad a las redes de pago para los comercios.

Tarjetahabiente
Portador de una cuenta Visa.

Comercio
Provee bienes y servicios a cambio de pago. Para aceptar tarjetas, los comercios deben de ser validados y mantener una relación con un Adquirente.

Los cuatro pilares de nuestra visión de seguridad

Devaluar la información sensible

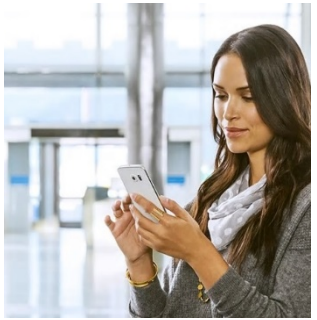
- ✓ Chip (EMV)
- ✓ Tokenización

Aprovechar tecnologías de datos (“Big Data”)

- ✓ Decisiones de fraude en tiempo real

Proteger los sistemas de información

- ✓ Evitar almacenar información sensible a nivel comercio



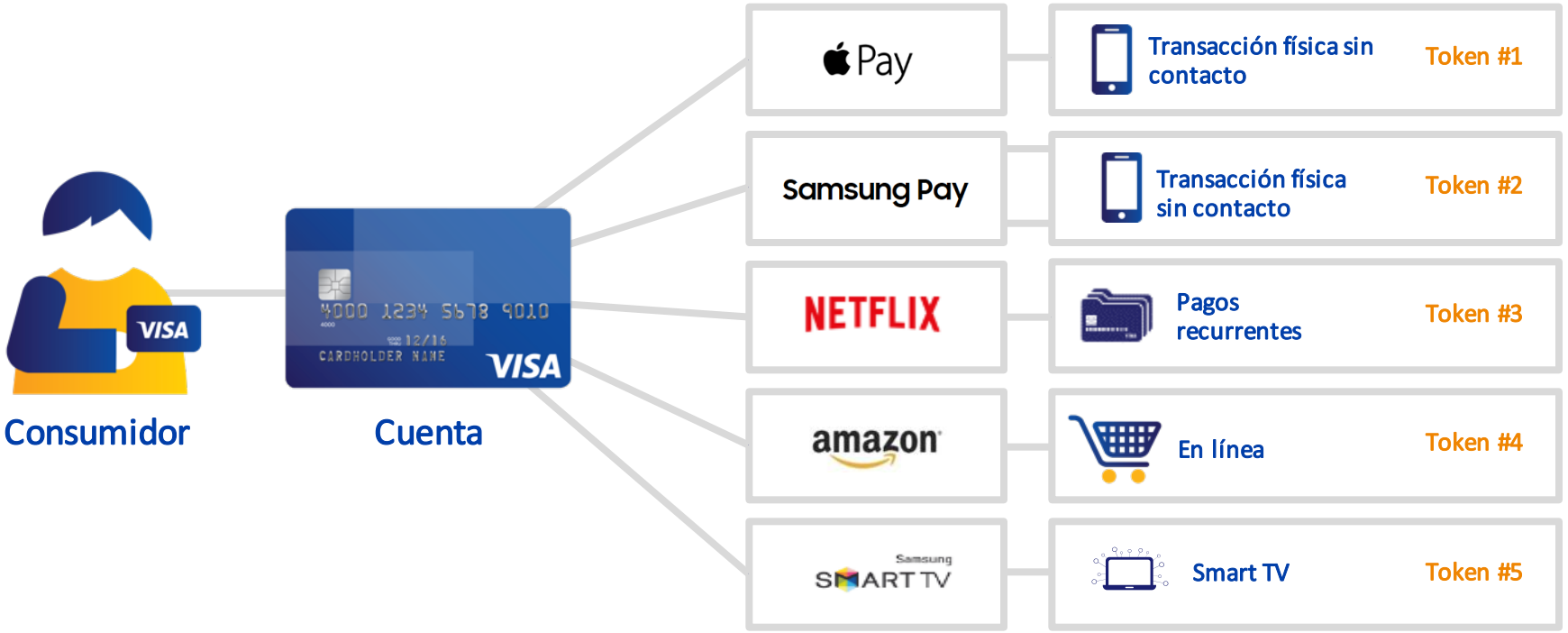
Proteger e involucrar al consumidor

- ✓ Alertas SMS o email
- ✓ “Cero responsabilidad”

Pilar #1 Devaluación de información - Chip

- Regla de cambio de responsabilidad
- Desde octubre 2014 el emisor o adquirente que no haya invertido y migrado a chip es responsable por el fraude
- Aplica en POS / ATM
- Cubre transacciones nacionales e internacionales

Pilar #1 Devaluación de información - Tokenización



Pilar #2 Uso de herramientas anti-fraude

Visa Rules 29 June 2017

Issuers Must Implement Fraud Prevention Tools

LAC | *Issuers, Processors*

Overview: To help issuers employ strong risk management strategies, and to foster consumer confidence in the payments system, Visa will require issuers in the LAC region to implement risk-scoring, real-time fraud prevention tools—and/or Visa Advance Authorization and Visa Risk Manager—for all products except prepaid by 21 July 2018.

As the card business has matured, so have fraudsters' techniques. This means issuers have to constantly review and improve their fraud management capabilities.

Having the right fraud prevention tool allows issuers to reduce fraud losses and increase authorization throughput by improving fraud detection and confidently approving low-risk transactions.

Visa is evolving and clarifying the Visa Rules related to risk tools,[1] and wants to ensure that each LAC issuer and/or its processor implements a risk-scoring, real-time fraud prevention tool—and/or Visa Advance Authorization (VAA) and Visa Risk Manager (VRM)—for all products except prepaid by **21 July 2018.**[2]

Mark Your Calendar:

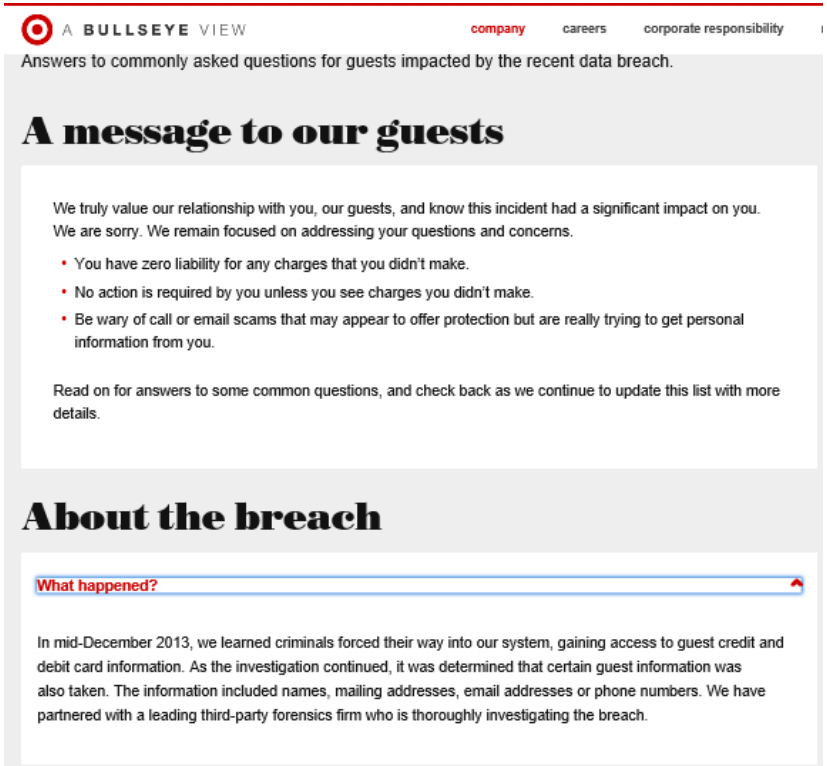
- Fraud prevention tool requirement for issuers takes effect **(21 July 2018)**

Related Training From Visa Business School:

- Fraud and Risk

A partir de julio 2018 todos los emisores requieren tener herramientas de monitoreo de fraude en tiempo real

Pilar #3 Salvaguarda de la información



A BULLSEYE VIEW company careers corporate responsibility

Answers to commonly asked questions for guests impacted by the recent data breach.

A message to our guests

We truly value our relationship with you, our guests, and know this incident had a significant impact on you. We are sorry. We remain focused on addressing your questions and concerns.

- You have zero liability for any charges that you didn't make.
- No action is required by you unless you see charges you didn't make.
- Be wary of call or email scams that may appear to offer protection but are really trying to get personal information from you.

Read on for answers to some common questions, and check back as we continue to update this list with more details.

About the breach

What happened?

In mid-December 2013, we learned criminals forced their way into our system, gaining access to guest credit and debit card information. As the investigation continued, it was determined that certain guest information was also taken. The information included names, mailing addresses, email addresses or phone numbers. We have partnered with a leading third-party forensics firm who is thoroughly investigating the breach.

- Caso Target en EEUU como ejemplo de los riesgos de robos de información a nivel comercios
- Desarrollo de estándares de industria (PCI-DSS) para evitar estos ataques
- Programas de cumplimiento
- Responsabilidad del comercio en evitar almacenar información sensible del medio de pago

Fuente: https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ

Pilar #4 Involucrar al tarjetahabiente

Alertas

- Obligación a emisores de ofrecer a tarjetahabientes Visa opción de notificaciones y alertas
- Email, SMS, llamadas, etc.
- Comunicado diciembre 2016
- Efectivo octubre 2017

Protección del Tarjetahabiente

- Regla de “cero responsabilidad”
- Busca proteger al consumidor pero generando responsabilidad
- Nace en EE.UU. y se expande gradualmente a nivel global
- Aplica en América Latina y el Caribe desde agosto 2016

Principio de “cero responsabilidad”

Beneficios a tarjetahabiente

- NO es responsable por cargos no autorizados siempre y cuando:
  - i. No haya autorizado la transacción
  - ii. No haya participado de la transacción
  - iii. No se haya beneficiado de la transacción

Alcance

- Casos de robo, extravío y fraude
- Todos los canales (POS, ATM, en línea, etc.)
- Transacciones nacionales e internacionales
- No aplica en cierto productos (comerciales, prepago anónimo)

Obligación del emisor

- Abono provisional dentro de cierto plazo de tiempo dependiendo de tipo de producto
- Conduce investigación con adquirente
- Define si hubo o no responsabilidad del tarjetahabiente y/o el comercio
  - ✓ El comercio puede tener responsabilidad bajo ciertas circunstancias, incluyendo, colusión con defraudadores, no envió transacción para autorización, no siguió el proceso para una transacción con chip, robos de información, etc.

El reto de la seguridad en los pagos

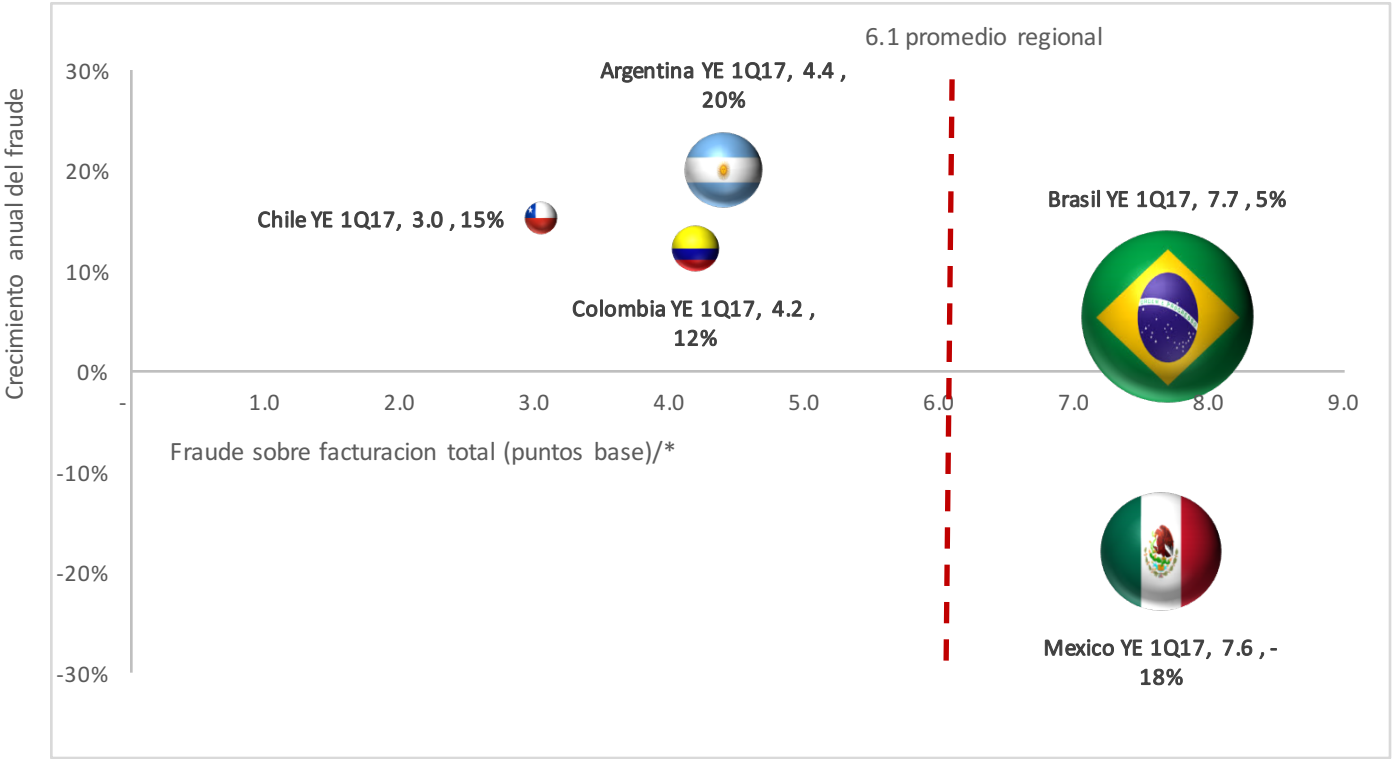
Conveniencia

Cliente

Seguridad

Datos

El fraude en Chile se mantiene bajo



/* Facturacion total incluye POS y ATM. Tamaño de la burbuja refleja el monto total relativo para cada país
Fuente: Visa Inc, Reporte TC 40 enviado por los emisores

Consideraciones finales

- Hoy en día hacer pagos de manera electrónica es más segura y conveniente
- Visa y sus emisores y adquirentes invierten sumas crecientes en materia de tecnología y herramientas de seguridad
- Las reglas y protocolos que establecemos van dirigidas a generar incentivos para que todas las partes involucradas en la cadena de pagos asuman su responsabilidad
- El principio de “cero responsabilidad” para el consumidor es un beneficio que conlleva obligaciones de un uso responsable del medio de pago
- El Proyecto de reforma a la Ley 20.009 que se revisa en el Senado (Boletín N° 11.078-03) busca ampliar la protección del consumidor financiero pero es importante hacerlo de manera integral y atendiendo responsabilidades para todos los participantes

Sugerencias

- Diferenciar rol emisor de rol adquirente u operador en línea con las definiciones de la nueva normativa de tarjetas de pago del Banco Central de Chile

    - ✓ Operador o adquirente como entidad responsable de la vinculación con el comercio (afiliación, interconexión, liquidación de transacciones, etc.)

- En el articulo 6 establecer que “El usuario no se tendrá por responsable en las operaciones realizadas sin su autorización, ***siempre y cuando dicha operación se le haya previamente reportado al emisor [...]”***

- En el artículo 7 (a) incorporar el concepto de “abono provisional” sujeto a los resultados de la investigación en lugar de “cancelación de los cargos” o “devolución de los importes” y (b) considerar un plazo que no exceda de cinco días en lugar de 24 horas.

- En el caso del comercio establecer obligaciones de salvaguardar y proteger la información de los usuarios así como de colaborar en las investigaciones

Gracias