2020 Global CX Forum
24° CONGRESO MÉXICO

Fraude en el CC y los Canales Digitales

Carlos Vazquez
Director Regional

NUANCE

imt.

2020 Global CX Forum
24º CONGRESO MÉXICO

Tendencias que transforman el fraude en el centro de llamadas

Las pérdidas por fraude son enormes

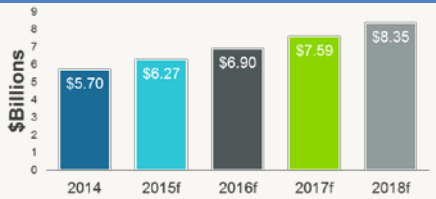
U$S 17,5 mil millones robados por fraude en 2017 (más de U$S 1,5 mil millones)

Las pérdidas por apropiación fraudulenta de cuenta (ATO) contribuyeron en U$S 5,1 mil millones al fraude general

1,5 millones de consumidores fueron víctimas de fraude tanto de Apropiación Fraudulenta de Cuenta (ATO) como de Nueva Cuenta (NAF)

Y siguen creciendo

Tasa de crecimiento anual compuesta del 10%



16,7 millones de consumidores estadounidenses víctimas de robo de identidad o fraude de identidad en 2017

6,64% de los consumidores fueron víctimas de Fraude de Identidad (en comparación con el robo de identidad)

Estafadores con miras al centro de llamadas

U$S 2,16 mil millones perdidos en centros de llamadas ante. U$S 1,08 mil millones perdidos en aplic. móviles

Una de cada 1200 llamadas a centros de contacto de empresas es una llamada fraudulenta

El 70 porciento del fraude en el centro de llamadas es perpetrado por los mismos delincuentes.

NUANCE

Javelin Strategy and Research 2017, Bank InfoSec, Aite Group, informe Agari, Forbes

imt

El fraude en el contact center y los canales digitales.

Contact centers: el talón de Aquiles de la prevención del fraude

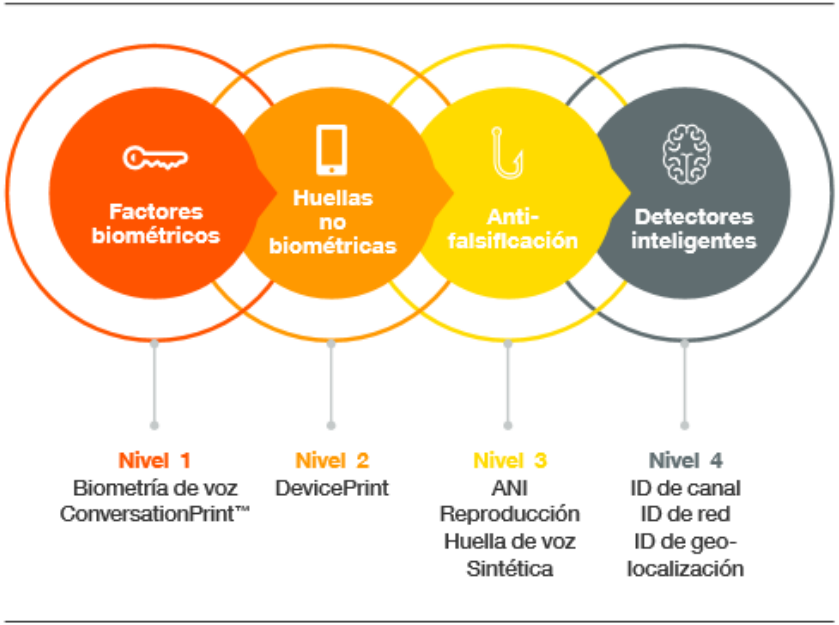
El fraude está aumentando en todos los canales de interacción con el cliente, bien se trate de servicios financieros, agencias gubernamentales, telecomunicaciones o compañías aéreas. Pero los expertos están de acuerdo: el *contact center* es quizás el canal más vulnerable y el objetivo más fácil para los ladrones.

Los contact centers se han convertido en los «epicentros de vulnerabilidad en muchas organizaciones».1
Gartner

2020 Global CX Forum
24° CONGRESO MÉXICO

El fraude en el contact center y los canales digitales.

Estrategias para encontrar el equilibrio entre detección y prevención y la experiencia del cliente.



NUANCE

imt.

2020 Global CX Forum
24° CONGRESO MÉXICO

Capas de defensa contra el fraude

- Identificación de canal
- Identificación de red
- Identificación geográfica - Lista ANI

- Validación ANI
- identificación de
- Memoria
- Sintética

- DevicePrint

- Biometría de voz
- ConversationPrint™
- Otros datos biométricos

NUANCE

imt.

Capas de defensa contra el fraude

Indicadores Inteligentes

- ID de canal – analiza el audio para determinar el tipo de canal (línea fija, móvil, VOIP/web)
- ID de red – analiza la calidad de transmisión de audio (pérdida de paquetes, latencia, calidad de voz perceptiva)
- Identificación geográfica – analiza la información geográfica asociada con ANI (operador, país, ciudad, tipo de medio)
- Lista ANI – permite la creación, el filtrado y la toma de decisiones en base a listas blancas y negras
- Todos los indicadores son *complementarios* ta al reconocimiento de voz biométrico

Identificación de canal
Identificación de red
Identificación geográfica - Lista ANI

Validación ANI
identificación de
Memoria
Voz

DevicePrint

Biometría de voz
ConversationPrint™
Otros datos biométricos

Capas de defensa contra el fraude

Antifalsificación

- Validación de ANI – detecta los intentos de falsificación y bloqueo de ANI (70-80% de precisión)
- Reproducción/Memoria – algoritmos que detectan el audio grabado/reproducido
- Voz sintética – algoritmos que detectan ataques mediante voz sintética.
- Todos los indicadores son *complementarios* ta al reconocimiento de voz biométrico

Identificación de canal
Identificación de red
Identificación geográfica - Lista ANI

Validación ANI
identificación de
Memoria
Voz

DevicePrint

Biometría de voz
ConversationPrint™
Otros datos biométricos

Capas de defensa contra el fraude

Impresiones no biométricas (NBP)

- Analiza características de audio únicas de un dispositivo específico
- Crea y almacena una "impresión" que se compara durante las llamadas posteriores
- El desajuste se utiliza como un indicador de compromiso (IOC)
- *Complementario* al reconocimiento de voz biométrico (+14%)

Identificación de canal
Identificación de red
Identificación geográfica - Lista ANI

Validación ANI
Reproducción
Memoria
Voz sintética

DevicePrint

Biometría de voz
ConversationPrint™
Otros datos biométricos

Capas de defensa contra el fraude

Factores biométricos

- Biometría de voz - competencia básica de Nuance; precisión insuperable; (líder en innovación industrial durante más de 20 años, 4ta generación de redes neuronales profundas (DNN)
- ConversationPrint™ – analiza la selección de palabras, la gramática y la estructura de las oraciones (10% más de detección de fraude, 34% menos de alertas falsas en comparación con la biometría de voz)
- Otros datos biométricos – fichas biométricas adicionales (huella dactilar, rostro, comportamiento)

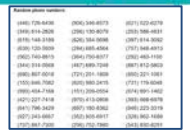
Identificación de canal
Identificación de red
Identificación geográfica - Lista ANI

Validación ANI
Reproducción
Memoria
Voz sintética

DevicePrint

Biometría de voz
ConversationPrint™
Otros datos biométricos

Motor de inteligencia artificial de seguridad: conexión de datos



Validación ANI

Identificación geográfica

identificación de canal

Identificación de red

DevicePrint

Motor de inteligencia artificial de seguridad

Salida

Puntuación de autenticación: 97,15

Puntuación de riesgo: 6,55

Conversation Print™

Factores biométricos

2020 Global CX Forum
24º CONGRESO MÉXICO

Ciclo de ataque de fraudes

Reconocimiento
- Acceso vía telefónica u online
- Validar datos
- Obtener saldo
- Comprobar la higiene financiera
- Determinar el ataque

Configuración
- Crear nuevo beneficiario
- Cambiar dirección
- Solicitar tarjeta de reemplazo
- Solicitar recordatorio de PIN
- Restablecer los detalles de inicio de sesión
- Transferencia interna de fondos
- Solicitud de préstamo
- Aplicación de sobregiro
- Etc.

Adquisición de datos
- Dark web
- Phishing, Smishing, Vishing, etc.
- Empleados corruptos
- Hacking de emails
- Virus
- Intercepción postal

Retiro de dinero
- Realizar el pago
- Transferencia de saldo
- Cualquier tipo de mov. de dinero

Acceso a fondos limpios
- El estafador recupera el dinero

Blanqueo de dinero
- Movimiento entre cuentas "limpias"
- Movimiento offshore
- Uso de cuentas "mulas"

Con Nuance Security Suite se identifican a los estafadores al interactuar en el centro de contacto. Típicamente en las etapas 2, 3 y 4.

La detección de fraudes en las etapas 2 o 3 impide que llegue a la etapa 4, la etapa en la que se ponen en riesgo el dinero o los activos.

La etapa 4 es donde la detección en tiempo real se vuelve más importante.

Es posible utilizar Security Suite para evitar que el fraude llegue a la Etapa 4, la etapa de "Retiro de dinero".

imt.

Cambio de deflexión por fraude a persecución por fraude

12

Juicios fraudulentos exitosos donde VB fue utilizado como evidencia

Biometría de voz para detección de fraudes

Hace…

Identifica llamadas fraudulentas que permiten tomar medidas correctivas.

Permite revelar la verdadera escala del fraude

El análisis permite identificar a los estafadores más prolíficos.

Puede ayudar a revelar la verdadera identidad del estafador

Biometría de voz para detección de fraudes

Nuance ofrece…

Automatización para reducir significativamente los procesos intensivos de trabajo

Aprendizaje automático/IA para reducir FPs/FRs y priorizar alertas

Integración con herramientas y procesos existentes.

Control (caja blanca) de IOCs, relaciones FP/FR y hora

Alianza que ofrece experiencia, conocimiento y consultoría

imt.

2020 Global CX Forum
24º CONGRESO MÉXICO

Case de Estudio: Pensiones Banorte

- 98% aumento en CSAT
- 95% resolución en la primera llamada (FCR)
- 98% en niveles de autenticación
- 24/7 disponibilidad inmediata

"La satisfacción del cliente ha aumentado drásticamente como resultado de la implementación de la biometría de voz. Iván Aguirre, Director de análisis y canales alternativos de pensiones Banorte

BANORTE | PENSIONES

imt.

2020 Global CX Forum
24° CONGRESO MÉXICO

Case de Estudio: Pensiones BBVA Mexico

- Mayor satisfacción del cliente al simplificar el proceso y hacerlo más fácil.
- Se redujo el flujo de clientes que entran en las sucursales para transacciones simples.
- Involucruan a los clientes a través de tecnologías digitales fáciles y seguras.
- Rápida adopción: más de 70.000 clientes se inscribieron en 11 meses.

BBVA

imt.

Nuance le ahorra $ 24 millones costos durante 3 años para un banco multinacional Fortune 100

[El impacto económico total de Nuance Security Suite](), Junio de 2018

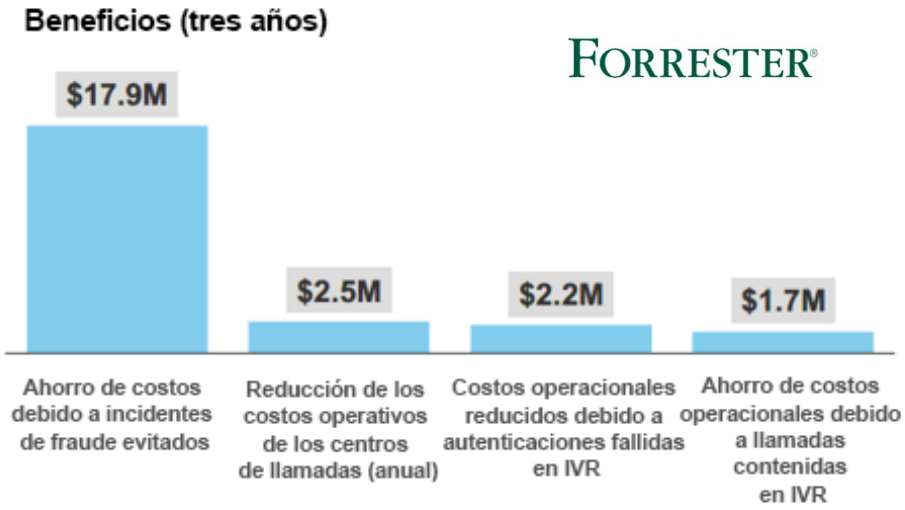
Banco multinacional Fortune 100

U$S 24 millones

En ahorro de costos durante 3 años.

191%
ROI (retorno de la inversión)

10
Mes de amortización



Forrester Research, El impacto económico total de Nuance Security Suite, Junio de 2018

2020 Global CX Forum
24° CONGRESO MÉXICO

Implementación de Nuance Security Suite:

Web

- Autenticación avanzada
- Canal de inscripción biométrica.
- Mitigación de fraudes

Móvil

- Autenticación avanzada
- Inicio de sesión de aplicación alternativa
- Canal de inscripción biométrica.
- Mitigación de fraudes

IVR

- Reemplazo de PIN para autoservicio
- Factor de autenticación para el centro de contacto.
- Mitigación de fraudes

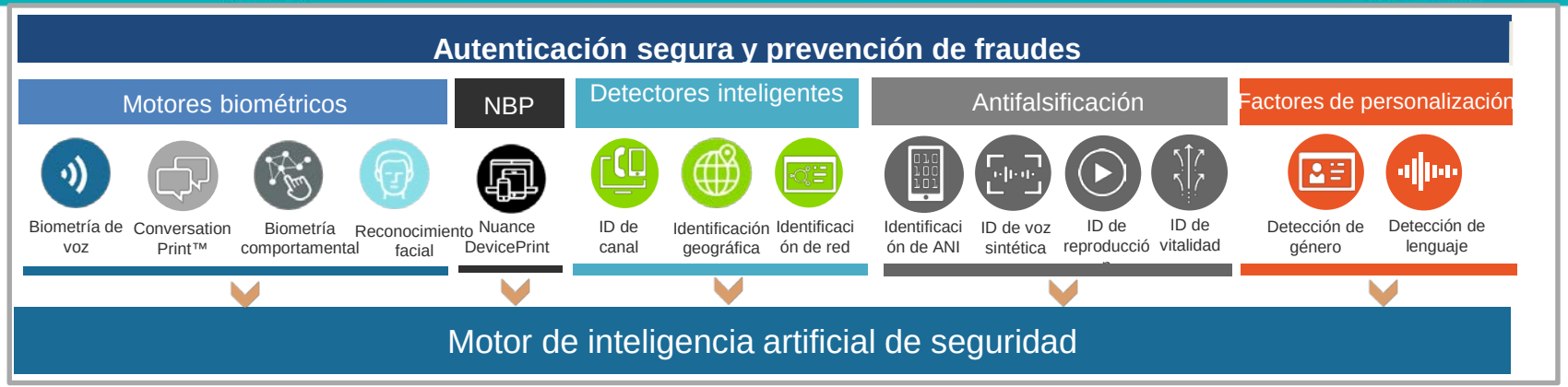
Centro de contacto

- Reemplazo de cuestiones de seguridad
- Mitigación de fraudes

imt.

2020 Global CX Forum
24° CONGRESO MÉXICO

Características generales de Nuance Security Suite:



Conexión uniforme: Los clientes se autentican de forma transparente con cero esfuerzo y por cuenta propia

Canal cruzado y dispositivo: Los clientes pueden autenticarse con la misma credencial en todos los canales y dispositivos

Preparada para el futuro: Security Suite protege contra futuros vectores de ataque, como los ataques de voz sintética

¿Alguna pregunta?