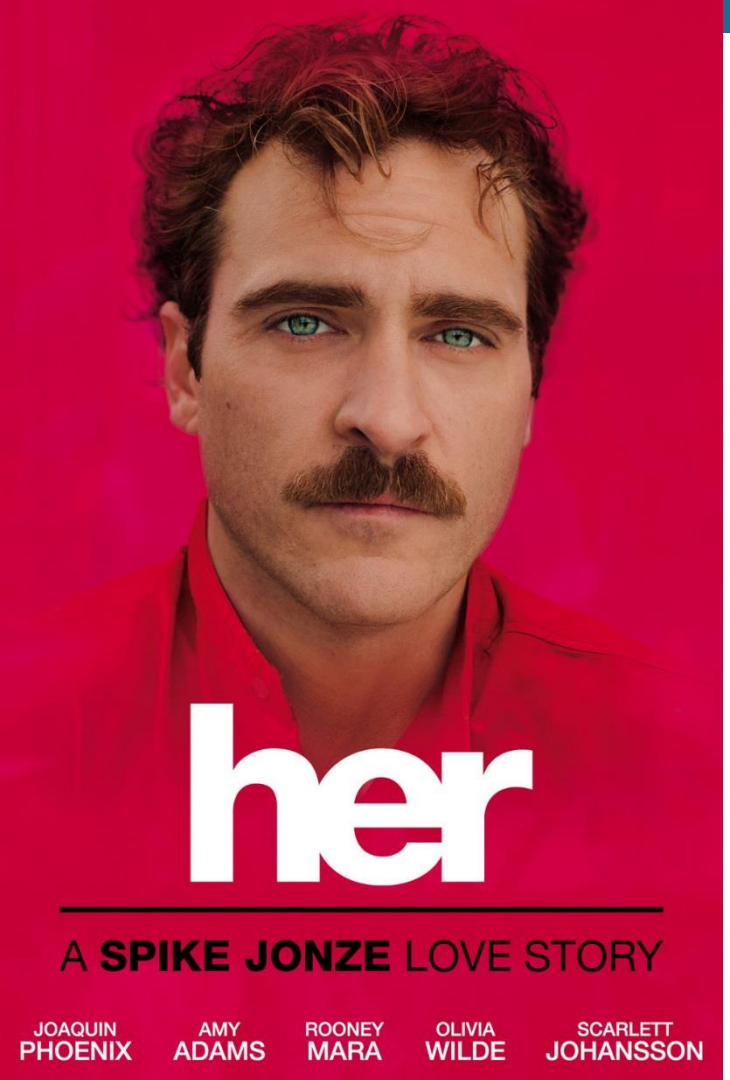
Voice, Face and Behavioural Biometrics

Authentication & Fraud Prevention in the age of Virtual Assistants

Brett Beranek, Director Product Strategy, Biometrics, Security & Fraud



Our interactions with technology and organizations will become **seamlessly personalized**.

It will feel like the devices, applications and organizations we interact with know who we are, **like a friend** does when they hear our voice or see our face.

Our identities will be known and validated through various **biometric** modalities, determined by interaction preference.

Nuance Security Suite,
replacing PINs, passwords, and
security questions.

Voice Biometrics
Return on Investment Data

51%

increase in NPS score

39%

increase in self-service usage

59%

decrease in account takeover within 30 days of deployment

TATRA BANKA
Member of RZB Group

Manulife

Top 5 UK Bank

NUANCE

Voice Biometrics
Impacts on Retention and Sales

Customer retention

57%

reduction in customer churn within contact center

Upsell

143%

increase in upsell rate

156%

increase in average upsell value

NUANCE

Authentication Failure Rates

IVR
41% authentication failure rate

Smartphone
96% make mistakes typing passwords

Web
37.4% of shopping cart abandonments occur at login

Source: Coleman Parkes Research in close conjunction with both Opus and Nuance, 2013

Consumer Frustration and Acceptance of Conversational / Intelligent Self Service

90%

Would prefer voice biometrics over passwords or questions

89%

Prefer conversation with virtual assistants over search

73%

Prefer personalized conversations

83%

Want an alternative to PINs and passwords

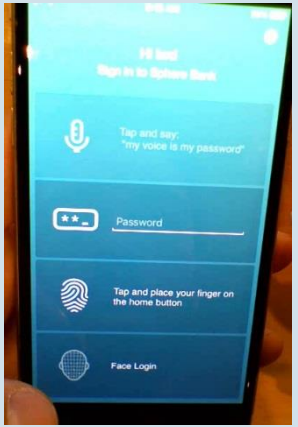
NUANCE

Consumers Split over Biometric Modalities

Preferred Authentication Modality for Mobile Application Access

Method	% Preferred
Fingerprint	40%
Face	30%
Voice	25%
Password	5%

Study participants were instructed to enroll and verify with 4 separate authentication modalities.



KATE CALDWELL
INTERACTION EXPERIENCE

NUANCE

Voice Most Reliable Mobile Authenticator
but not appropriate for all contexts

Authentication Success Rate

Method	Verification Success
Voice	**100%**
Password	90%
Fingerprint	80%

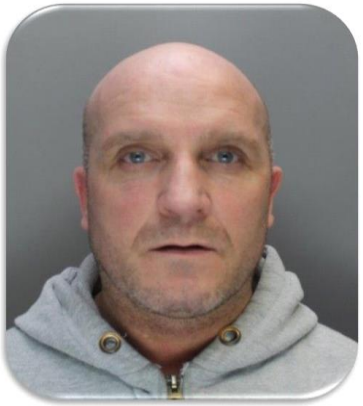
Yet, other factors drive preference

“Let's say I am sitting on the bus, I wouldn’t wanna use my voice as my password, repeating that... it would sound weird.”

Provide Law Enforcement with Identifying Evidence

Voice biometric evidence is actively being used by enterprises to identify fraudsters and to support the arrest and prosecution of fraudsters by providing identifying evidence to law enforcement.

NUANCE



Sentenced to 2 1/2 years

Name: Lee Chisholm

Age: 44

Chisholm repeatedly made call pretending to be the customer gathering personal information to allow him to take control of accounts. He then used the cards to make a variety of purchases which he would sell on. He specialised in garden furniture, Christmas hampers and hairdressing products.

Using voice biometrics, we managed to track his exploits preventing £370,000 of financial loss

Sentenced to 7 years

Name: Maxwell Parsons

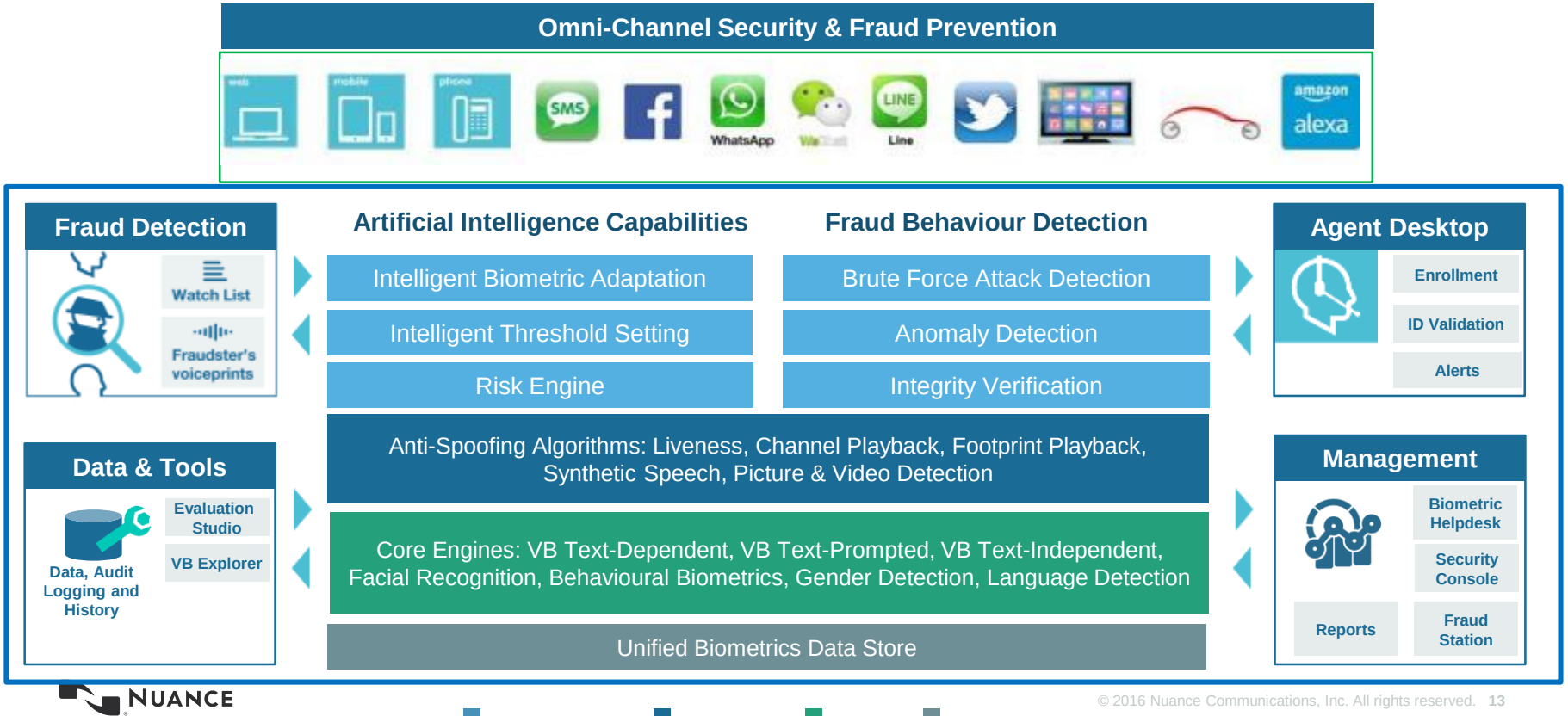
Age: 49

Defrauded the banking industry of £2.5m

Parsons devised computer software to reverse bank transactions enabling him to spend money repeatedly from a number of Banks. At the peak of their activities, police said the gang had "laundered" up to £50,000 a day.

Nuance Security Suite

Security & Fraud Prevention for All Channels



Key Takeaways

- When biometrics are seamlessly woven with virtual assistants, a personalized and conversational interactions is delivered to consumers
- This human-like experience drives customer retention and increased revenue
- Fraud benefits alone can justify investment in biometrics

NUANCE

Thank you