

20 November – 2:15 p.m. – 3:00 p.m.

Optimizing Authentication Performance in Multifactor Solutions

Speaker:

- **Chuck Buffum**, VP, Caller Authentication Solutions, Nuance



NUANCE

The experience speaks for itself.™

Optimizing Multifactor Authentication

chuck.buffum@nuance.com



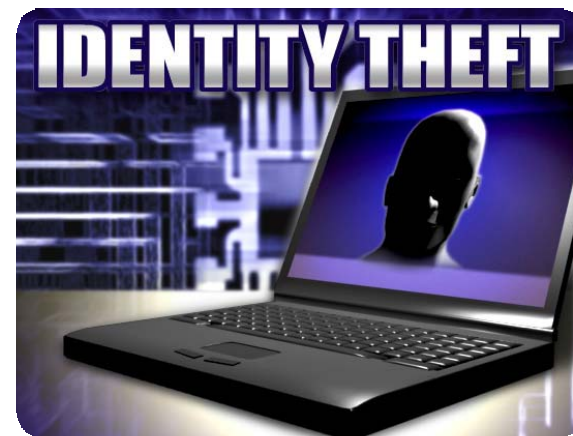
Agenda

- Profiling risk in the call center
- Key components in MFA solutions
- Configuring MFA solutions to meet business objectives
- Optimizing MFA performance
- Realistic performance expectations

Identity Theft vs. Fraud

Identity Theft is Step One

- The acquisition of identity information – “the profile”
 - Lost or stolen computer tapes/disks
 - Computer virus attacks to collect bulk data
 - Mail theft or dumpster diving
 - Phishing
 - Pre-texting, social engineering, etc.
- Step one in the criminal process
- Often goes un-noticed for weeks or months
- Criminal underground in place to buy/sell profiles



Identity Theft vs. Fraud

Fraud is Step Two

- Using the profile to steal assets from the victim
 - Account takeover fraud
 - High volume, lower loss per incident
 - Average = \$1000
 - New account fraud
 - Lower volume, higher loss per incident
 - Average = \$10,000
- Strong movement from internet fraud to phone fraud
 - Most FIs implemented multi-factor authentication in past 3 years



Current Call Center Authentication is Exposed

IVR-based Authentication

- 4 digit PIN
- Can ignore or bypass to get to agent authentication

Agent-based Authentication

- Two to four questions from the following (>90%)
 - Mother's maiden name
 - Last 4 digits of SSN
 - Date of Birth
 - Zip Code
- These weak “tokens” protect the high risk transactions



How Weak Are These Tokens?

- **Genealogy Sites Provide a Good Starting Point**

- Search by name and approximate age & location
 - Location & date of birth
 - Parent's names & their wedding date
 - Grandparent's name, yielding Mother's maiden name
- Wedding and birth information is in the public record



- **Investigator Sites For Those Who Need Fast Access**

- Merlindata.com – just one example
 - \$10 per month – promise not to misuse the information
 - Reverse phone number lookup (full address & zip code)
 - Business & credit profiles, often full SSN



Trained User Can Build Complete Profile in Less Than 3 Minutes!

Agenda

Key components in MFA solutions

Authentication components

- Identity Claim
 - Memorable, but not too private
 - Usable as index into customer database
- Authentication Process
 - Layered authentication mapped to perceived risk
 - Multi-factor, yet streamlined
 - Primary authentication – should handle 90%+ of calls
 - Voiceprint + ANI or Content
 - Secondary authentication – should handle @5% of calls
 - Additional factor, liveness testing, etc.
- Enrollment process
 - Secure process for pre-enrollment authentication
 - Rich enough for good voiceprints, fast enough for high completion rate

Management components

- Credential (voiceprint) database
- Authentication logging
- OA&M tools
- Audit & compliance reporting
- Risk management interface
- Fraud investigation interface

Configuring MFA solutions to meet business objectives

Balancing the Business Objectives

- Risk & Security
 - Stronger, multi-factor authentication
 - Data available for compliance reporting, fraud investigations, etc.
- Customer Service & Marketing
 - Streamlined call (faster & easier)
 - Possible differentiation in service level, privacy, or personalization
- IT & Operations
 - Compatible with existing infrastructure
 - Supportable, extensible, etc.

Standard business-level performance metrics

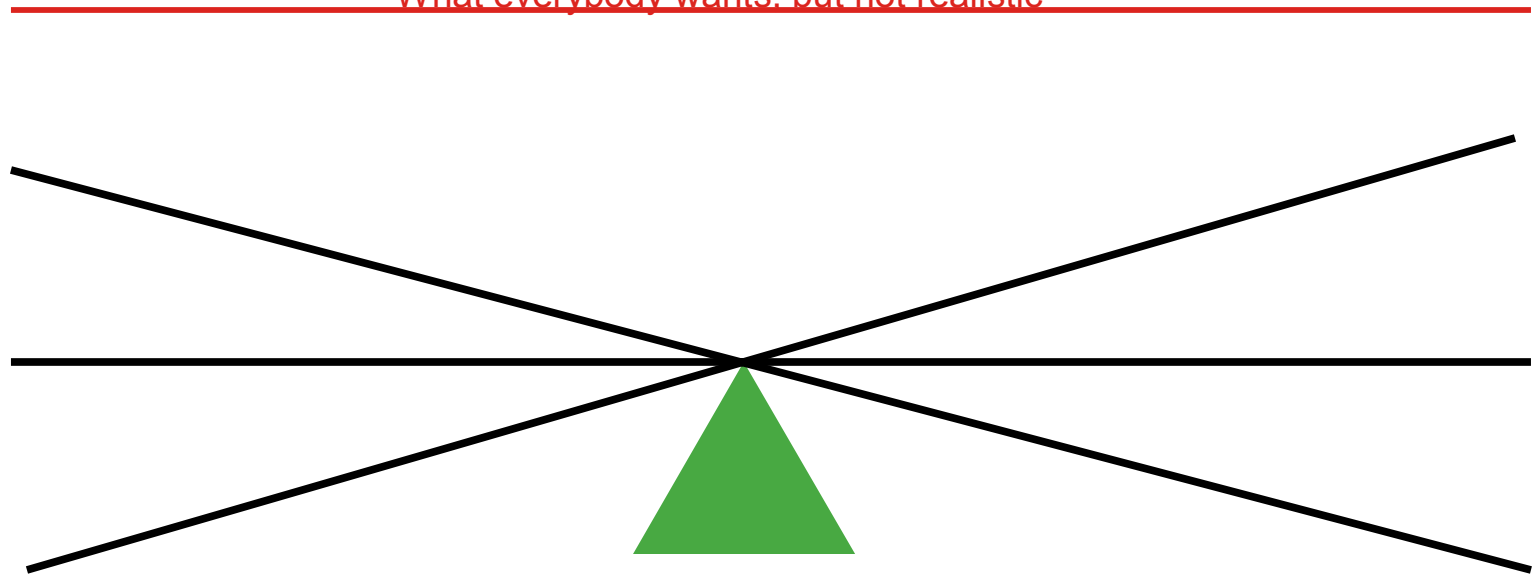
- Correctly Automated Authentication rate
 - Measures the percent of callers successfully passing through caller verification within the application
- Enrollment Success rate
 - Measures the percent of callers able to successfully enroll in the service
- Transaction Security Rate
 - Measures security level during imposter testing
 - $TSR = 1 - \%FA$
 - Combines both biometrics and other factors like knowledge verification

Security & Convenience tradeoffs

High Security

High Convenience

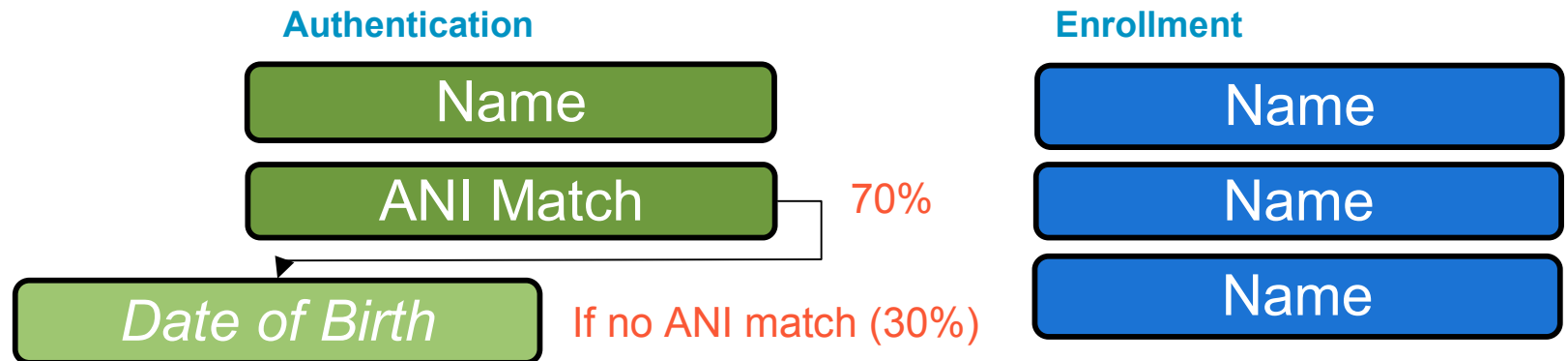
What everybody wants. but not realistic



Low Security

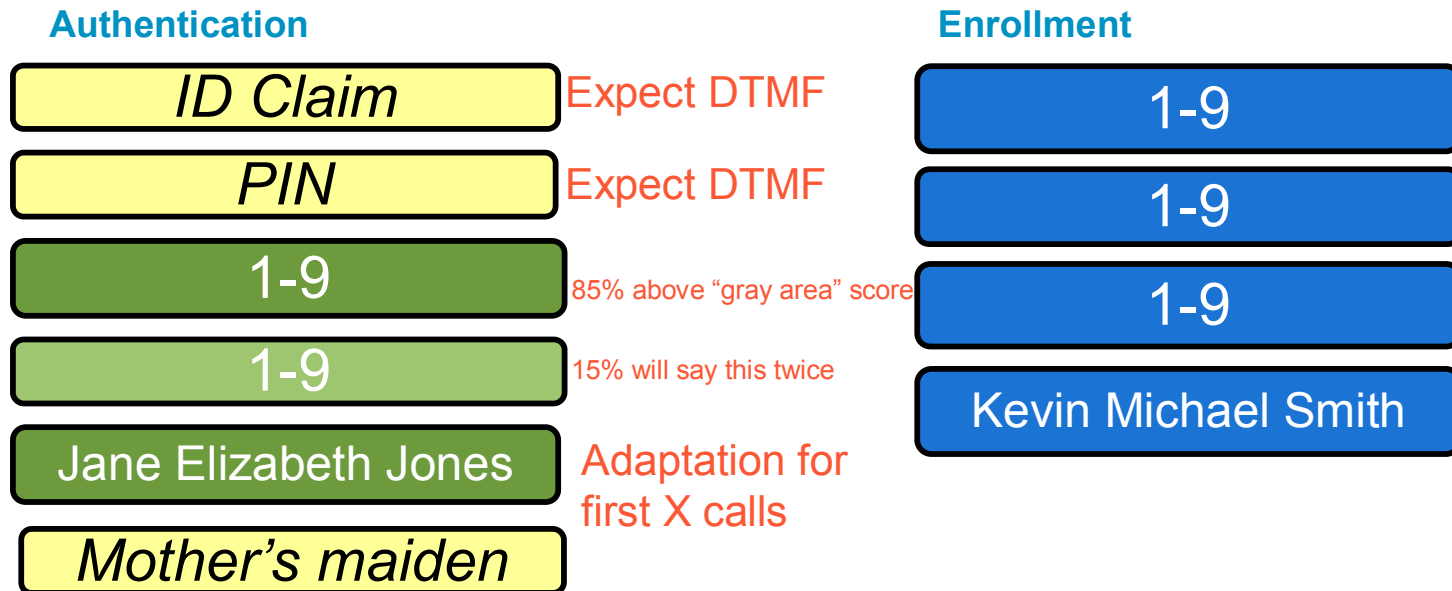
Low Convenience

High convenience, low security: “Say your name”



- Fast enrollment and authentication
- May work well for employee facing systems with name grammars
 - The name IS the identity claim – Identification and Authentication in one step
- If name grammars are not available an identity claim would need to be added to the dialog. “What is your ID?” Name is still used for the biometric
- Text Dependent Verification provides high accuracy
 - Longer names are more secure
 - “My full name is” as an intro adds phonetic info to voiceprint
- Missing liveness testing

High security, low convenience: Add biometrics to existing authentication



- Text Dependent Biometric adds highest biometric security to existing security flow
- Text Independent/Similar Biometric adds liveness testing
 - Higher security is achieved on this pass due to specialized Text Independent enrollment and ongoing adaptation
- Dialog is secure but cumbersome with two biometric tests and two knowledge verification tests

Balanced security and convenience

Authentication

Account Number

Account Number

KV (Secret Date)

85% above "gray area" score

15% will say this twice

Enrollment

Account Number

Account Number

Account Number

KV (Secret Date)

- Text Dependent Biometric brings high biometric security
- Knowledge Verification ensures multi-factor authentication
- Convenient: Many callers will complete in two utterances
- Single step Authentication and Verification with Account Number
 - Requires an account number that people are willing to speak out loud
 - Substitute a passphrase for sensitive accounts. (A separate identity claim is needed in authentication dialog)

A few thoughts on “Liveness” Testing

- A “Liveness Test” can be incorporated to defend against fraud attacks which use a recording of the true caller
- Liveness Tests generally ask the caller to speak a phrase which is different from call to call
 - Recognizer ensures the person is saying the right thing
 - Verifier matches the voice to the voiceprint
- Liveness Tests make recording attacks more difficult, but add an extra step for true callers which may reduce call automation
- Considerations:
 - Likelihood of a recording attack
 - Risk or the sensitivity of the transaction to be performed
 - Combination with other factors in the authentication dialog

Agenda

Optimizing MFA performance

Factors influencing voice biometric performance

- Richness of voice enrollment
 - Broad phonetic coverage
 - Deep phonetic coverage (3x)
- Quality of audio sample
 - SNR
 - Completeness of utterances
- Environmental characteristics
 - Channel mismatch
 - Speaker health, background noise, etc.

Optimizing voice biometric performance

- Leveraging ASR features
 - Maximize enrollment quality
 - Utterance clipping
 - SNR
 - Channel detection
 - Maximize interpretation of voiceprint score
 - Complete & correct utterance spoken?
 - SNR
 - Channel detection – allows compensation for mismatch
 - Automated voiceprint adaptation (threshold based)
- Most effective liveness testing
 - Both what was said and who said it (Text Similar Verification)

Realistic performance expectations

Real World Performance

- Set realistic business objectives
 - +/- 10% of users unwilling to engage – no matter what you do!
 - Build business case on 80% success
 - Layered authentication mapped to perceived risk
 - Multi-factor, yet streamlined
- For compliant callers
 - Primary authentication – should handle 90%+ of calls
 - Voiceprint + ANI or Content
 - Secondary authentication – should handle @5% of calls
 - Additional factor, liveness testing, etc.

Reference – TD Waterhouse

- Identity Claim = spoken phone number
 - Recognizer used to validate
- Primary Authentication Process
 - Voiceprint score (TD) on phone number utterance
 - Content matching on “secret date”
- Secondary Authentication Process (DTMF phone number or poor score)
 - Voiceprint score (TD) on “my voice is my password”
 - Content matching on secret date
- Enrollment process (Agent performed pre-enrollment authentication)
 - Speak phone number 3 times
 - Say “my voice is my password” 3 times
 - Say secret date (speech enrolled grammar) & record hint
- Resulting Performance
 - Correctly automated authentication > 95% (compliant users >80%)
 - FA = 0.4% , FR = 4.3% (fall back to manual auth.)

Summary

- Synthesize the business objectives
- Design solution to achieve proper balance of security & convenience
- Leverage the best practices & lessons learned
 - Risk rules & security architectures from secure online systems
 - Layered, multi-factor authentication
 - Security schemes are never “final” – threats keep changing
- Leverage the technology to maximize automated authentication
- Collaborate with other early adopters to share best practices
- Assemble the best team to help you deploy