Optimizing call center authentication: Balancing fraud control with the customer experience
"It looks like everyone will be getting what they want this year... somebody posted my credit card number on the internet!"
Optimizing call center authentication

- Introductions and common challenges
- Existing authentication techniques
- Client shared best practices
- Emerging authentication technologies
- Q&A
Introducing:

- Stefan Schubert
  JPMorgan Chase & Co

- Bobbie Paul
  Experian

- Roger Bouvier
  Experian
Call center authentication challenges

Target activities
- Credit line increase and money transfers
- Travel notifications
- PIN or password reset
- Address changes

Human factor
- Trained to provide excellent service
- Deal with exception cases
- Good intentions preyed upon

Cross-channel Fraud schemes
- Email and text to access accounts
- Multiple attempts across different channels
- Social engineering
Existing authentication techniques

Roger Bouvier
Optimizing call center authentication
Existing authentication techniques

- Knowledge-based authentication
- Risk-based decision models
- One-time passwords
- SMS text
- Outbound phone
“…news of my death has been greatly exaggerated.”

— Mark Twain
Knowledge-based authentication (KBA)

KBA in today’s call center
- Static vs. dynamic KBA
- Component is a layered authentication strategy

KBA challenges and benefits
- Applicable to a large number of consumers
- Customer friction
- Impact of data breaches
“We adore chaos because we love to produce order.” — M. C. Escher
Risk-based decision models

The pros and cons
- Frictionless customer experience
- Greater efficiency
- Impact of data breaches

What to look for in a risk model provider
- Quality and freshness of data
- Performance against industry benchmarks
- Ability to provide custom models

Relevance of risk-based decisioning
- Still applicable in today’s call centers
- Customer experience
- Next generation risk scores
How do one-time passwords fit into an authentication strategy?

- Layered approach to authentication
  - Mitigates impact of data compromises
- Level of assurance strategies
  - Removes reliance on static passwords

Benefits of using one-time passwords via SMS text

- No need for physically mailed tokens or hardware
  - Reduces operational expense
- Deploy across large user base
  - Improved customer experience
Outbound calling

How do outbound calls fit into a authentication strategy

- Manage suspicious behavior or high risk populations
- Complimented by phone or device intelligence

Benefits and challenges of using an outbound call strategy in a call center

- Provides greater control in higher risk situations
- Increases potential for customer friction
- Increase to operational expense
Call center authentication best practices

Stefan Schubert
Call centers are not a growth industry, but they are not going away.
Overview and approach methodology

Call centers are the “end of the line” for customer problems

- Manage complex failure scenarios

Data-based approach to losses and customer experience

- Treat authentication as a transaction
- More than just procedures and questions

Where science fails, use art – logically tackling authentication problems

- Driving customer behavior
- The ability and will to say “no”
Trends in attack

Multi-factor vs. multi-source authentication
Public digital lives coupled with data driven approach by fraudsters enables account takeover at will

Customer victimization to phishing makes static dangerous
Change for the sake of change is good!

Compromise of third party products increase risk of unorthodox attacks
Phone forwarding, text intercept and man in the middle style phone attacks increasing in frequency
Rise in data breaches enable rapid growth in attack rate

- Mixed KBA more effective than single source KBA

Authentication strategy doesn’t stop when the call ends

- Customer alerting
- Using authentication data downstream

Matching the authentication to the request

- Authentication that compliments the service
Emerging authentication technologies

Bobbie Paul
Technology changing the landscape
New and re-emergence

Phone print
Better than voice authentication

Document verification
New technology keeping this as the last resort

Biometrics
Is there enough trust?
Phone printing

The leverage
- Convert phone print
- Insert opt-in; no voice capture
- High fraud capture; low false positive

The encumbrance
- Regulatory compliance
- Early adoption
- Integration into processes and procedures
Documentation

The leverage

- Technology enables real-time review
- No longer a subjective review
- Provides that ‘last resort’ authentication option

The encumbrance

- Expense
- Friction and customer satisfaction
- Regulatory; storage and retention
Biometrics

The leverage
- Distinguish between white and black lists
- Reduced handle time

The encumbrance
- Security; once compromised it cannot be changed
- Low success rate of usable voice prints captured
- Low adoption
  - Provides that ‘last resort’ authentication option
Thinking beyond tomorrow

The leverage

- By 2020, estimated 80% of consumers will have smart phones
- Consumers trust and use biometrics for authentication increasing
- Additional layers of authentication and consumer choice

The encumbrance

- Security; once compromised, cannot be changed
- System connectivity, internal platforms and communication
- Regulatory stance unknown
For additional information, please contact:

Roger.Bouvier@experian.com

Bobbie.Paul@experian.com

Follow us on Twitter:

@ExperianVision | #vision2016
Share your thoughts about Vision 2016!

Please take the time now to give us your feedback about this session. You can complete the survey in the mobile app or request a paper survey.

1. Select the Survey button and complete
2. Select the breakout session you attended
VISION 2016
TAKE CONTROL
A ROADMAP FOR GROWTH

©2016 Experian Information Solutions, Inc. All rights reserved.
Experian Public.
#vision2016