Voice Authentication On-Demand: Your Voice as Your Key

Paul Watson, Vice President
Relationship Technology Management

Voice Search Conference
March 2-4, 2009
Convergys Corporation
A Global Leader in Relationship Management

**Worldwide Capabilities**
- 75,000 employees
- 85 customer and employee contact, service and data centers worldwide; focused on optimizing employee and customer experience
- Clients in 70+ countries speaking nearly 35 languages

**A Leading Public Company**
- $2.8 billion in revenues
- Listed on NYSE, S&P 500, Fortune 1000
- A *Fortune* Most Admired Company for eight consecutive years
- Serve more than half of the Fortune 50 as clients

**Key Facts About Convergys**
- Host more than 1 billion customer interactions annually
- Support more than 3 million employees and retirees worldwide
- Billing for 350+ million communications subscribers worldwide
- Named to the Top 10 for Innovative Use of Technology by *InformationWeek* (2007)
On-Demand Voice Authentication - Agenda

- Market Overview: Needs & Dynamics
- Voice Authentication Flash Demo
- Business Drivers: security, cost, revenue
- On-Demand Voice Authentication Infrastructure
- Live Demo
- Conclusion
Voice Authentication Market Dynamics

- Consumers are experiencing increasing concern about security and identity theft.

- Governing agencies are providing guidelines and requirements for multi-factor authentication:
  - Banking (FFIEC)
  - Medical (HIPAA)

- Voice authentication can now be leveraged in IVR, web, and agent transactions.

Voice Authentication Adoption Hurdles

Voice authentication technology is ready, but traditional deployment:
- ...takes too long,
- ...requires capital expenditure,
- ...and has required a speech IVR.
Increase in Phone-based Fraud

- “Mail and phone-based incidents rose dramatically, from 3% of ID fraud in 2006 to 40% in 2007”

- “As consumers shift more financial transactions to secure online arenas, fraudsters have become more creative in utilizing land and wireless telephones to access information”

- “Address changes are among the most popular methods of attack. A criminal may call and claim he wants to change the address on an account. Using stolen data to verify his identity, he may gain access without ever possessing a card.”

2008 Identity Fraud Survey Report:
Identity Fraud Continues to Decline, But Criminals More Effective at Using All Channels
February 2008
Voice Authentication Market – Gartner & OPUS

OPUS Key Findings
- Voice biometric solutions are maturing
- $80M in 2006 → ~$800M in 2011

Factors propelling growth
- Evolution of technology → products
- Integration with existing infrastructure
- Multiple pricing and delivery options
- Password reset proves its value
- Enrollment has not been a problem
- Mandates for strong authentication
- Gov’t will drive large deployments
- Mobile users to drive next apps

Gartner Key Findings
- 60% of banks plan to strengthen authentication
- >50% of online banking consumers consider extra security features "extremely" important.
- 23% of online banking consumers think answering challenge questions is a waste of time.

Recommendations
- Implement non-PC-based user authentication for high-risk, online transactions.
- Implementing secret questions to verify callers significantly adds to call center costs.
- Consider voice biometrics for stronger caller authentication.
<table>
<thead>
<tr>
<th>Why should you Use VA?</th>
<th>Why will customers adopt VA?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meet Industry Guidelines</strong></td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>❖ Regulatory support for technology</td>
<td>❖ Belief that identity theft is a threat</td>
</tr>
<tr>
<td>❖ FFIEC Multifactor Authentication “Guideline”</td>
<td>❖ Perception that biometrics work</td>
</tr>
<tr>
<td>❖ VA is a fit for 2nd factor</td>
<td>❖ Acceptance of voice over other biometrics</td>
</tr>
<tr>
<td>❖ Contact center cost savings</td>
<td></td>
</tr>
<tr>
<td>❖ Reduce AHT</td>
<td></td>
</tr>
<tr>
<td>❖ Automate PIN/PW reset</td>
<td></td>
</tr>
<tr>
<td><strong>Employee Applications</strong></td>
<td><strong>User Experience</strong></td>
</tr>
<tr>
<td>❖ Ensures security for company sensitive information</td>
<td>❖ Voice authentication reduces or the need to remember a PIN/password</td>
</tr>
<tr>
<td>❖ Lower cost for secure transactions</td>
<td>❖ VA saves time compared to answering challenge questions.</td>
</tr>
<tr>
<td></td>
<td>❖ Contributes to greater mobility</td>
</tr>
</tbody>
</table>

© 2008 Convergys Corporation. All rights reserved.
Voice Biometrics – Ready for Prime Time

Pros:
- Equivalent in accuracy to Eye Scans and Fingerprints
- Low cost implementation; incremental to pre-existing IVR investment
- Non-invasive: uses a familiar mode of interaction → speech
- Easy to integrate with IVR apps; supports both phone or POS use
- Can be utilized across channels (Live-agent, IVR, Web and Mobile)
- Can combine with behavioral data to improve overall performance

Cons:
- Must deal with channel & device distortions
- Must manage user performance and perception, anywhere, on any phone

Sources:
Drivers for On-Demand Voice Authentication

- **Card Issuer: Reduce Fraud**
  - **Pain Points**
    - Customer Fraud; e.g., change of address, funds transfer
    - Agent time for authenticating callers
  - **Use Case Profile**
    - Enroll customer at card activation
    - Include VA for some/all call transactions
  - **Business Case Drivers**
    - Reduce existing fraud: 90%+
    - Reduce agent AHT: 10+ sec.
    - ROI: <6 months

- **Health Insurer: Gain Revenue**
  - **Pain Points**
    - Only 10% of new “enrollees” sign/mail policy
  - **Use Case Profile**
    - Allow policyholders to enroll & use “voice signature”
    - Use for HIPAA-compliant transactions
  - **Business Case Drivers**
    - Increase sales rate closure
    - Saves 9:1 in processing
    - Accelerates policy renewal anniversary
Client Benefits of an On-Demand VA Solution

- **Software as a Service**
  - No capital expenditures; pay-as-you-go pricing
  - No speech or biometric software for client to install
- **High-availability web services-oriented architecture**
  - Fast Implementation for Customers
  - Allows seamless interface from IVR and Agent applications & platform

**Customer Authentication Infrastructure**

- **Phone**
- **Mic**
- **Device**

**Convergys On-Demand Voice Authentication Infrastructure**

- Voice Authentication Application Intelligence

**Applications**

- DTMF or Speech IVR
- Any Web Based Application
- Multi-Modal Device Applications
Convergys Value Prop

- Deployment Benefits
  - Make it easy and fast to implement
    - From any IVR or Web app
  - Apply CVG’s expertise in large-scale hosting
    - Quick to market and low cost
  - Offer Voice Authentication Service On-Demand
    - High-available, scalable

- Technology Benefits
  - Core technology is robust, but need applications
    - Differences are in:
      - Business rules on top of Voice Authentication
      - Ease of integration and deployment
      - User interface design and sophistication
  - CVG – Labs has vetted vendor products and services over the past four years
Voice Authentication Business Value Drivers

- **Operational Cost Savings**
  - Reduce AHT via automated authentication

- **Fraud**
  - Reduce fraudulent transactions

- **Retention**
  - Increase customer satisfaction
  - Retain higher percentage of customers

- **Marketing**
  - Grow customer base via promotional marketing
    - “you’re secure with us”

- **Sales**
  - Increase close rate by offering immediate contract
  - Drive wallet share to increase card usage and revenue
Voice Authentication Use Case Demos

- **Demo 1 (Flash)**:
  - Two factor Authentication – userID/Password + Voice
  - Three modes of user interaction
    - Outbound phone call to user
    - Inbound phone call from user
    - Access from PC

- **Demo 2 (Flash)**:
  - Multi-modal and Multi-channel interface
    - Voice authentication from a multimodal PDA
    - Out-of-band voice authentication – voice unlocks access to web

- **Demo 3 (Live)**:
  - Control access to secure financial transactions with VA
  - Seamless Integration with IVR application
On-Demand Voice Authentication: Ready for Launch

- The Market appears poised to consume voice authentication

- Convergys brings agent, multi-channel, and large-scale hosting

- Convergys Advantages:
  - One Stop Voice Authentication solution
  - Complementary Customer Service solutions
  - Automated Self-Service
  - Complementary business decisioning software
  - Live agents
Questions, Comments, Insights?
Appendix

Voice Authentication: Performance Metrics
Voice Authentication Market – Gartner - June 2008

Key Findings

• To authenticate online banking customers, most U.S. banks rely on desktop cookies, and secret questions and answers. However, these recently deployed methods are already obsolete in the face of malware-based attacks.

• Most U.S. banks use weak methods to authenticate call center callers, but nearly 60% of surveyed banks plan to strengthen their authentication methods during the next two years.

• More than half of U.S. consumers consider extra security features "extremely" important in influencing their decision to bank online.

• Of the consumers who have to answer secret questions to bank online, 77% say they don't mind answering the questions, but the other 23% do, or they think the questions are a waste of time because they believe the questions provide little added security.

Recommendations

• Recognize that using secret questions and desktop cookies to authenticate online consumers raises the "security" bar, but those methods can be easily defeated by determined criminals.

• Start implementing non-PC-based user authentication and transaction verification for high-risk, online transactions. These methods can stop the damage from attacks launched from user browsers and desktops.

• Be cautious about implementing secret questions to identify call center callers — they may significantly add to call center operational costs.

• Consider automated PIN entry and/or voice biometrics for stronger caller authentication, although voice biometrics is still largely unproven in call centers with millions of customers.
Key Findings:
The market for voice biometric-based solutions is maturing, having generated nearly $80 million in licensing and application revenue in 2006. The market will grow modestly in the coming year, then grow to approach $800 million in revenue by 2011. Factors propelling growth include:

- **The evolution from “technology” to “products”** – For selected applications (like password reset) in specific enterprise settings (like contact centers and “Help Desks”) voice biometric-based authentication has proven value as a solution to well-defined problems.
- **Better interconnection and interaction with existing security infrastructure** – The product of greater acceptance by corporate security officers, as well as general IT implementers.
- **Support from larger integrators and resellers** – Larger firms, such as EMC’s RSA Security division and IBM Global Services, have added speaker verification to their range of products and services.
- **Multiple pricing and delivery options** – Solutions have moved beyond premises-based solutions (with pricing based on ports, servers or seats) to include hosted delivery of services driven by enrolled users and, ultimately, transactions.
- **Password reset (PWR) proves its value** – Deployments of this mainstay of speaker verification continue to grow as a result of more stringent security policy and the availability of “mature” solutions.
- **Enrollment has not been a problem** – Several firms that installed voice-based verification customer care contact centers have been pleased to find the large majority of callers choose to enroll.
- **Mandates for hardened authentication for financial services** – Largely driven by regulatory bodies in North America and Western Europe.
- **Largest deployments will be government-driven** – Consensus is building that voice biometrics will play an important role in making e-government services accessible and for hardening authentication where transfer payments are involved.
- **Mobile users to drive next wave of applications** – Access control for both employees and customers using mobile phones create readymade opportunities for speaker verification solutions.
Voice Authentication – Performance Metrics

- **Equal Error Rate**
  - Simple measure of performance
  - ~1% indicates high performance

- **Type I (FR), Type II (FA) errors**
  - Tradeoffs determine operating point
  - Good target:
    - type I: 0.5 – 1.0 %
    - type II: 1.0 – 3.0 %

- **Enrollability rate**: 
  - % of users who can be enrolled successfully
  - ~ 95% is an achievable goal

- **Verifiability rate**: 
  - % of users who can use the service with consistent success
  - ~95% is an achievable goal
  - ~5% of users may need alternate means (agent?)
Operational Analysis: Call Center Impact

- Voice Authentication can reduce current fraudulent calls by 98.9%
- Leverage authentication by alternative means in other 1.1% of calls
  - Additional questions built into the Voice User Interface
  - Live operators
  - Web-based questions for online applications

### Assumptions

<table>
<thead>
<tr>
<th>Assumptions</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total calls</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Fraudulent calls</td>
<td>0.05%</td>
</tr>
<tr>
<td>FAR</td>
<td>1.00%</td>
</tr>
<tr>
<td>FRR</td>
<td>1.00%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Call</th>
<th>Number of Calls</th>
<th>% of Total Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before VSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Genuine calls</td>
<td>999,500</td>
<td>99.950%</td>
</tr>
<tr>
<td>Fraudulent calls (falsely accepted)</td>
<td>500</td>
<td>0.050%</td>
</tr>
<tr>
<td>After VSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calls correctly accepted</td>
<td>989,505</td>
<td>98.951%</td>
</tr>
<tr>
<td>Calls correctly rejected</td>
<td>495</td>
<td>0.050%</td>
</tr>
<tr>
<td>Calls falsely accepted</td>
<td>5</td>
<td>0.001%</td>
</tr>
<tr>
<td>Call falsely rejected</td>
<td>9,995</td>
<td>1.000%</td>
</tr>
<tr>
<td>Totals</td>
<td>1,000,000</td>
<td>100.000%</td>
</tr>
</tbody>
</table>