

May 5 – 11:45 a.m. – 12:30 p.m.

Data Security and Information Services

Speakers:

- **Dan Elvester**, Director of Business Development, Experian
- **Kolin Whitley**, VP Fraud Solutions, TransUnion

Voice Biometrics - Experian



Market Overview

May 5, 2010



What the Market Needs

- Consumers are concerned about security
- Enterprises must balance security and customer satisfaction with cost
- Regulatory agencies require multi-factor authentication
- Consumers need to feel comfortable with any new technology



Current Authentication Methods

Within the large set of consumer authentication methods, Experian only offers KBA

Knowledge-Based Authentication (KBA)

- Knowledge-Based Authentication, Simple Passwords,
- Virtual Keypads, Improved Password Methods

Experian's Current Capability

Simple Token-Based Authentication

- Transaction Number Lists, Grid Cards

Software-Based Authentication

- Public Key Infrastructure (PKI) Credentials

Out-of-Band Authentication

- Short Message Service one-time-passwords (OTP), Out-of-Band (OOB) Authentication via Voice Telephony

Sophisticated Token-Based Authentication

- OTP Tokens, Smart Cards With Handheld Readers, PC-Connected Smart Tokens

Additional Safeguards to improve Confidence in User Authentication Decisions

- Customer Device Identification
- Transaction Anomaly Detection

Emerging Authentication Methods

- Biometric Authentication – Uses information extracted from unique physiological or behavioral traits to verify the asserted identity of a user

Two Factor Authentication Using Knowledge IQ

Challenge-response questions designed to be answered by the true consumer



Available standalone
or with scoring

Credit and noncredit
data assets and
questions

Flexible question
configuration and
decision strategies

Analytics and
performance monitoring

for

Authentication during
application

Account changes

Identity screening processes

Password resets

Account opening

Account activation

High-risk monetary and non-
monetary transactions

Fraud risk assessment prior
to relationship expansion

Integration of Voice Biometrics and Experian KIQ

- Enrollment – authentication prior to capture and use of voice prints
- Fail Safe – use KIQ when voice print fails or is not present
- High risk transactions – in addition to voice prints – KIQ can provide multi-level authentication
- Across the entire enterprise – extending the current technologies:
 - ◆ Password resets
 - ◆ Account activity
 - ◆ Notification services



Why Voice Biometrics and Experian KIQ

- Strong multi-factor authentication
- Identity protection – no need for passwords
- Consumer experience – common to ask questions
- Common experience – phone for voice biometrics
- Next level of authentication
- Combination of voice and knowledge
- Questions can be asked at any point in the authentication process
- Risk based approach to authentication
- Extension of current technologies



Biometrics Integration with Current Platforms

Two Factor Authentication



