

Trusted Identity of Providers in Cyberspace Hearing – July 11, 2012 Washington, DC

William R. “Bill” Braithwaite, MD, PhD, FACMI, FHL7
Chief Medical Officer
Anakam Identity Services
Equifax



› Fraud and Abuse

- Identity validation and verification, authentication, credentialing, relationship detection, and ongoing monitoring can limit risk and focus manual processing to prevent and detect fraud and abuse.

› Waste and Enablement

- Electronic Provider Identity enables administrative simplification and online automation to reduce costly manual processing.

› Privacy and Security

- Knowing provider identity with high assurance enables first responders in a disaster situation and increases trust that electronic health information exchanges are not being breached.

Identity Management Lifecycle

Registration

Verification

Proofing

Credentialing

Authentication

Access Management



- NIST Remote Registration Level 3 is the highest published standard for Remote ID Proofing. Requirements are:
 - *Verify* a government issued ID
 - *Verify* a financial account number
- Problems with this approach:
 - Driver's License– only 26 States Provide – ½ don't update
 - Data Breaches have made FI / PII Information Cheap –
 - Stolen credit card number - \$.40
 - Bank account numbers -\$10.00
 - credit card number + contact information - \$2.00
- LOA 4 Face to Face proofing with a notary public is more expensive and burdensome but not much more reliable given availability of fake IDs.

- Level 3 augmentation –examine dynamics and more data elements to segment risky identities to the highest granularity and accuracy:
 - Attributes
 - SSN Warnings – Deceased, Under-aged, and Issuance
 - Address Discrepancies and Risk Prone Locations
 - Criminal / Licenses / Watch Lists
 - Velocity
 - Repeated Field Level Submission To Company
 - Repeated Field Submission to Identity Provider
 - Repeated Claim or Access Submissions
 - Behavior
 - Credit Behavior Changes
 - Employment Status Change
 - Business / Individual relationship change or pattern
 - Unusual Transaction Pattern
- With more accurate segmentation of risky identities, you can find more of the fraud while auditing less of the population.

- › KBA Identity Proofing can be highly successful when available data and process:
 - Uses primary data sources that are fresh and accurate
 - Clearly binds information to a claimant
 - Is not readily available to others (out of wallet data)
 - Leverages unpredictability of attributes
 - Leverages data with coverage comparable to scope
 - Is guess resistant
 - Balances accuracy with fraud potential
- › Privacy – not collecting data, only confirming data already known
- › Still requires reliable manual process to deal with risky identities and conflict resolution
 - › Manual process can be well supported by real-time KBA interaction with examiner.

- › 1.5 million individual providers processed
- › 98% of credential records found for providers
- › 92% of providers processed without manual intervention within 3 months of program start
- › 9.6% of providers have criminal background information on record (speeding tickets to hard time)
- › 3000 ineligible providers identified and barred from the program in the first month
- › 270,000 provider organizations screened

› High Assurance Identity Proofing for Providers

- Best done remotely with KBA based on good data
- Need work on robust standards for KBA to enable broad identity trust federation
- Do it once, do it well, and trust (but verify)

› High Assurance Authentication for Providers

- Multiple mechanisms can be deployed for authentication in different situations/locations/risks, even for same individual.
- Do it often, do it well, adjust mechanisms dynamically based on potential risk while enabling efficient workflows.