FEDERAL RESERVE BANK of ATLANTA

BIOMETRICS: TECHNOLOGY AND POLICY ISSUES

Talk About Payments Webinar

Dave Lott
Retail Payments Risk Forum

James Loudermilk
IDEMIA National Security Solutions

October 29, 2020

CONNECTION INFORMATION

FEDERAL RESERVE BANK of ATLANTA

- **Webinar link**
  - https://www.webcaster4.com/Webcast/Page/577/37736
- **Choose to listen with your PC speakers**
  - If you are having trouble hearing through your speakers
    - Call-in Number: 888-625-5230
    - Participant Code: 4254 2100#
- **Ask a question**
  - Click the **Ask Question** button in the webinar tool.
  - Email rapid@stls.frb.org

TODAY'S PRESENTERS

James "Jim" Loudermilk
Senior Director, Innovation and Customer Solutions
IDEMIA National Security Solutions

Dave Lott
Payments Risk Expert
Retail Payments Risk Forum
Federal Reserve Bank of Atlanta

IDEMIA PROFILE

- 14,000+ employees, a global leader in identification doing business in 170+ countries with $3.2Bn in revenue
- Major supplier of payment cards and SIM cards, and trusted by more than 1,800 global financial institutions
- In US, the leader in ID systems, DL & ID, and enrollment

Public Safety Biometric

DMV Issuance

Enrollment Services

RETAIL PAYMENTS RISK FORUM

FEDERAL RESERVE BANK of ATLANTA

- We serve as a catalyst for collaboration in the consumer and commercial payments risk management arena. We:
  - Conduct research and provide analysis
  - Convene and share with interested parties
  - Promote actions to mitigate risk

Take On Payments weekly blog

- http://takeonpayments.frbatlanta.org

Retail Payments Risk Forum webpage

- https://www.frbatlanta.org/rprf

OUR DISCUSSION TODAY

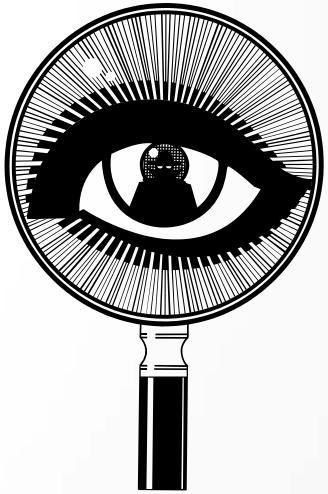
FEDERAL RESERVE BANK of ATLANTA

- Authentication
- Biometric Modalities
  - Fingerprint
  - Iris
  - Facial Recognition
  - Voice Recognition
  - Behavioral
- Enrollment Challenges
- Data Security
- Privacy
- Trust

IDENTITY AUTHENTICATION

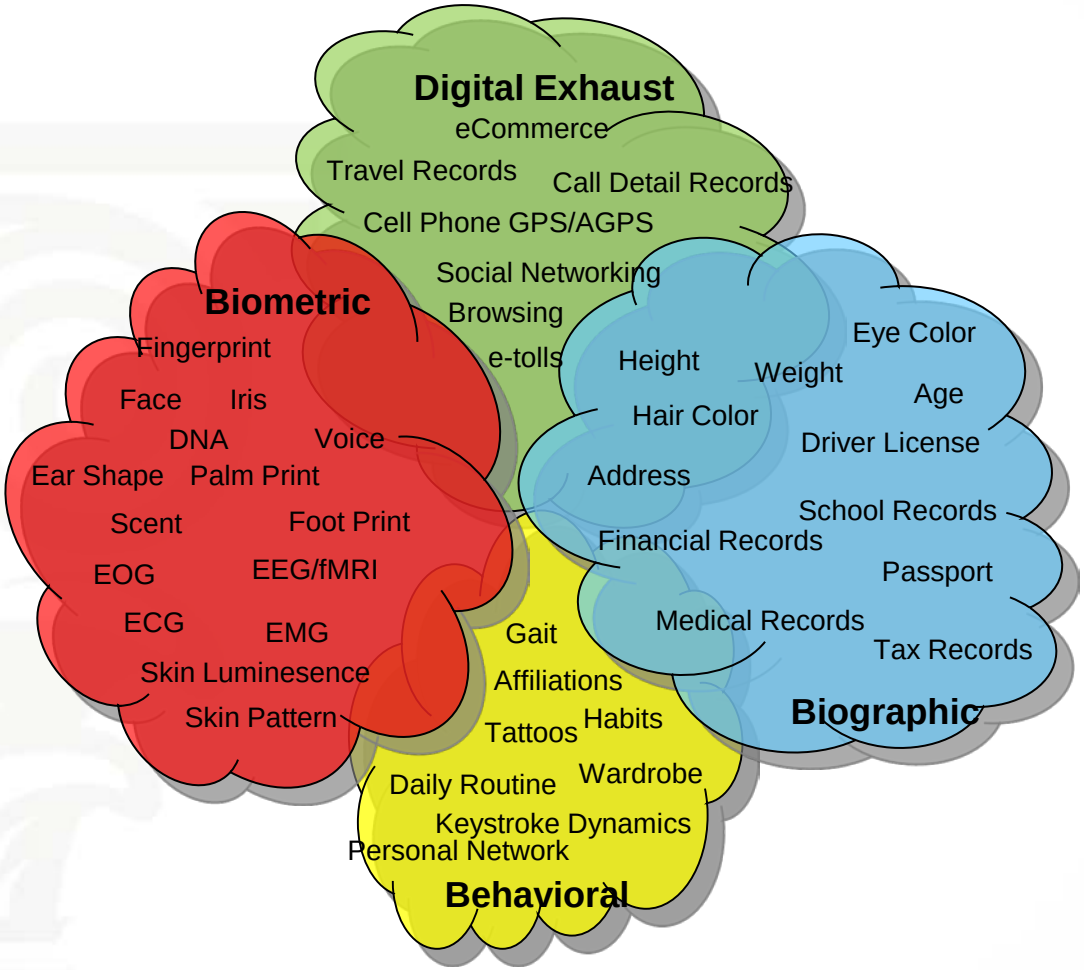
FEDERAL RESERVE BANK of ATLANTA

A Need as Old as Time



ELEMENTS OF IDENTIFICATION

FEDERAL RESERVE BANK of ATLANTA



HOW DO WE KNOW YOU?

FEDERAL RESERVE BANK of ATLANTA

Family/Friends/Colleagues:

When is the last time you asked to see identification? Never! You recognize them.

Travel, Federal, and Sensitive Facilities:

Commercial Activities:

Physical credentials serve many purposes and require much information. All that information is revealed – whether it's needed it or not!

ALL THESE CREDENTIALS

- Expensive to Produce
- Require Much Time to Obtain
- Reveal More Than the Officer/ Clerk Needs
- Highly Redundant Information
- Many Stewards Unable to Protect
- Ineffective in Cyberspace

ARE PHYSICAL CREDENTIALS EFFECTIVE?

FEDERAL RESERVE BANK of ATLANTA

(Is It Really You?)

- **Counterfeit Credentials**
- **Valid Credentials Fraudulently Obtained**
- **Biometrics Can "Fix" Identity**
  - Only you can be you
  - You cannot repudiate

AUTHENTICATION FACTORS

FEDERAL RESERVE BANK of ATLANTA

	Knowledge Factors (Something you know)	Possession Factors (Something you have)	Biometric Factors (Something you are)
	Information known to one entity and verifiable by another trusted entity	Tangible objects that cannot be readily copied or shared	Measurable biological or behavioural characteristics
Active (Requires customer engagement and participation)	• Passwords • PIN • Out-of-wallet questions known only to the verifying entity • Challenge questions	• Hardware tokens (e.g. USB) • One-time passwords (OTP) • Payment Card • Digital certificates • Driver's license	• Fingerprint • Voiceprint • Facial recognition • Iris pattern (eye scan) • Hand geometry
Passive (Can be done in the background, without customer's knowledge or engagement)		• PC/Laptop (IP) • Device fingerprinting	• Behavioral patterns • Facial recognition

REGULATORY GUIDANCE—FFIEC

FEDERAL RESERVE BANK of ATLANTA

"Since virtually every authentication technique can be compromised, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security…"

- **Supplement to Authentication in an Internet Banking Environment, 6/2011**

- Customer authentication should follow a risk-based approach
- **No single security solution covers all applications/transactions**

FINDING THE RIGHT BALANCE

- Security/risk versus customer experience
- Financial liability protection for consumers in the U.S. provides disincentive for consumers to adopt strong security practices

BIOMETRIC IDENTIFICATION

FEDERAL RESERVE BANK of ATLANTA

Twenty years ago, in a formulation that has stood the test of time, Anil Jain said:

"An ideal biometric should be ***universal***, where each person possesses the characteristic; ***unique***, where no two persons should share the characteristic; ***permanent***, where the characteristic should neither change nor be alterable; and ***collectible***, where the characteristic is readily presentable to a sensor and is easily quantifiable.

In practice, however, a characteristic that satisfies all these requirements may not always be feasible for a useful biometric system. The designer of a practical biometric system must also consider a number of other issues, including:

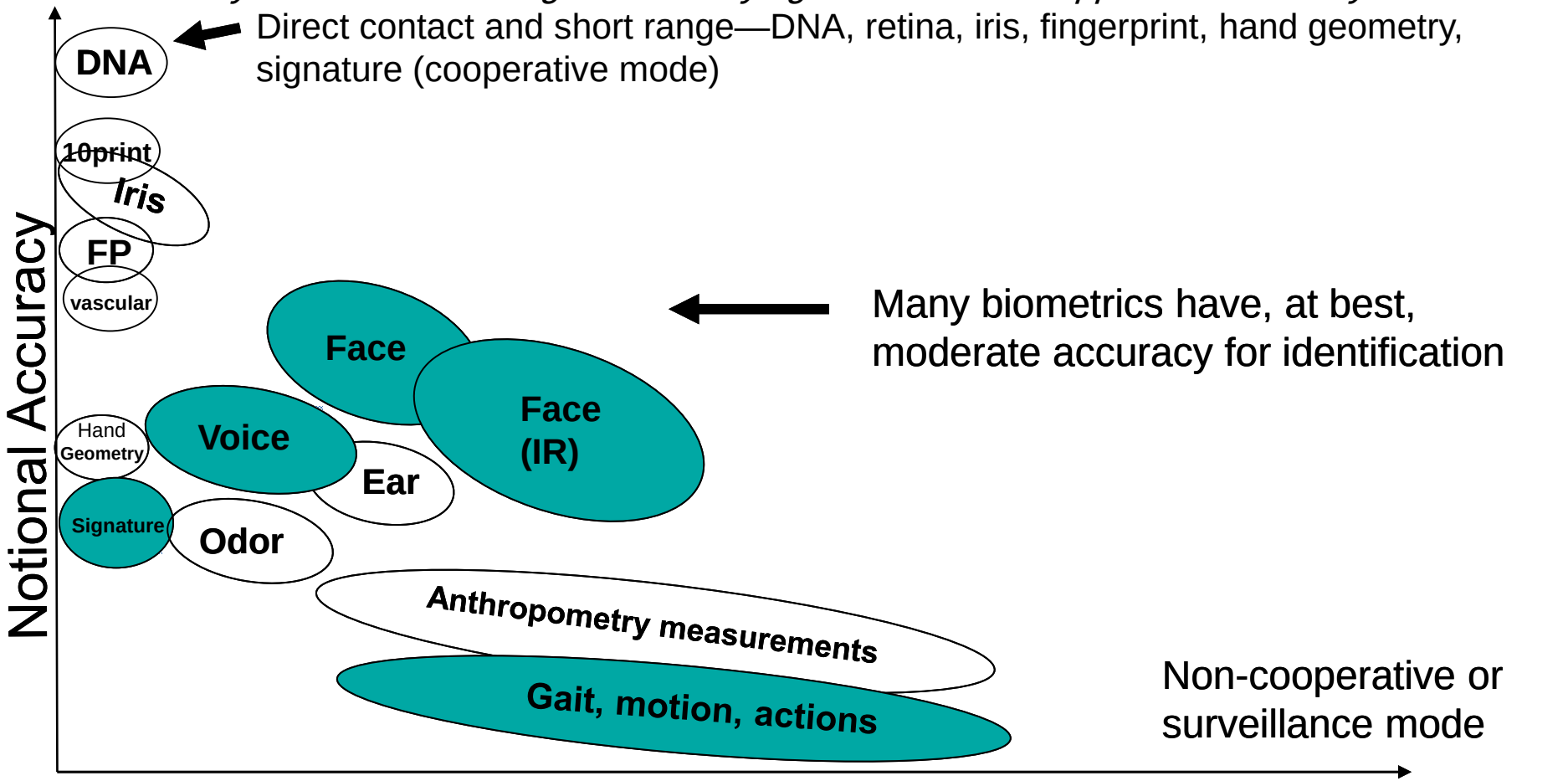
- *Performance*—that is, a system's accuracy, speed, robustness, as well as its resource requirements, and operational or environmental factors that affect its accuracy and speed;
- *Acceptability*—the extent people are willing to accept for a particular biometric identifier in their daily lives;
- *Circumvention*—how easy it is to fool the system through fraudulent methods."

TRADEOFFS IN SELECTING A BIOMETRIC

FEDERAL RESERVE BANK of ATLANTA

Many available technologies with varying levels of COTS application maturity

Direct contact and short range—DNA, retina, iris, fingerprint, hand geometry, signature (cooperative mode)



Many biometrics have, at best, moderate accuracy for identification

Non-cooperative or surveillance mode

Behavioral component

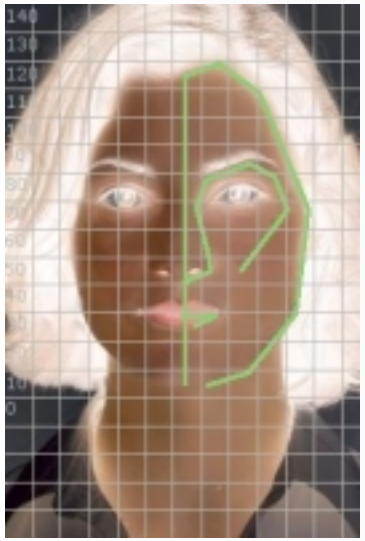
Slide concept Adopted from Human ID at a distance, Jonathon Phillips, NIST
(comments & notional placement of DNA—N. Orlans)

POPULAR PHYSICAL BIOMETRIC ELEMENTS

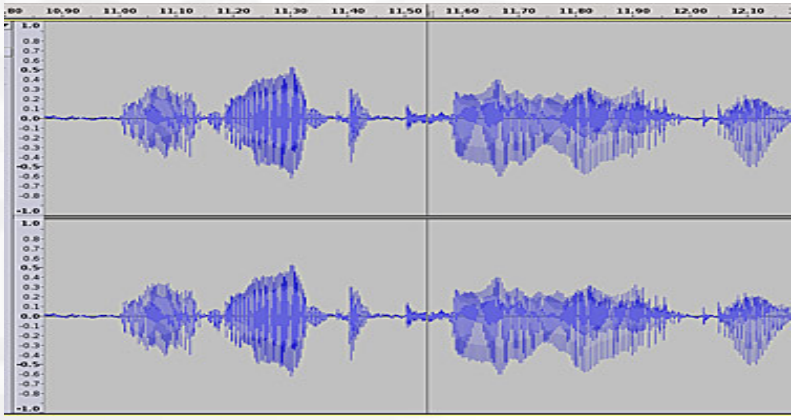
FEDERAL RESERVE BANK of ATLANTA

Finger / Palm Print

Iris Recognition



Facial Recognition



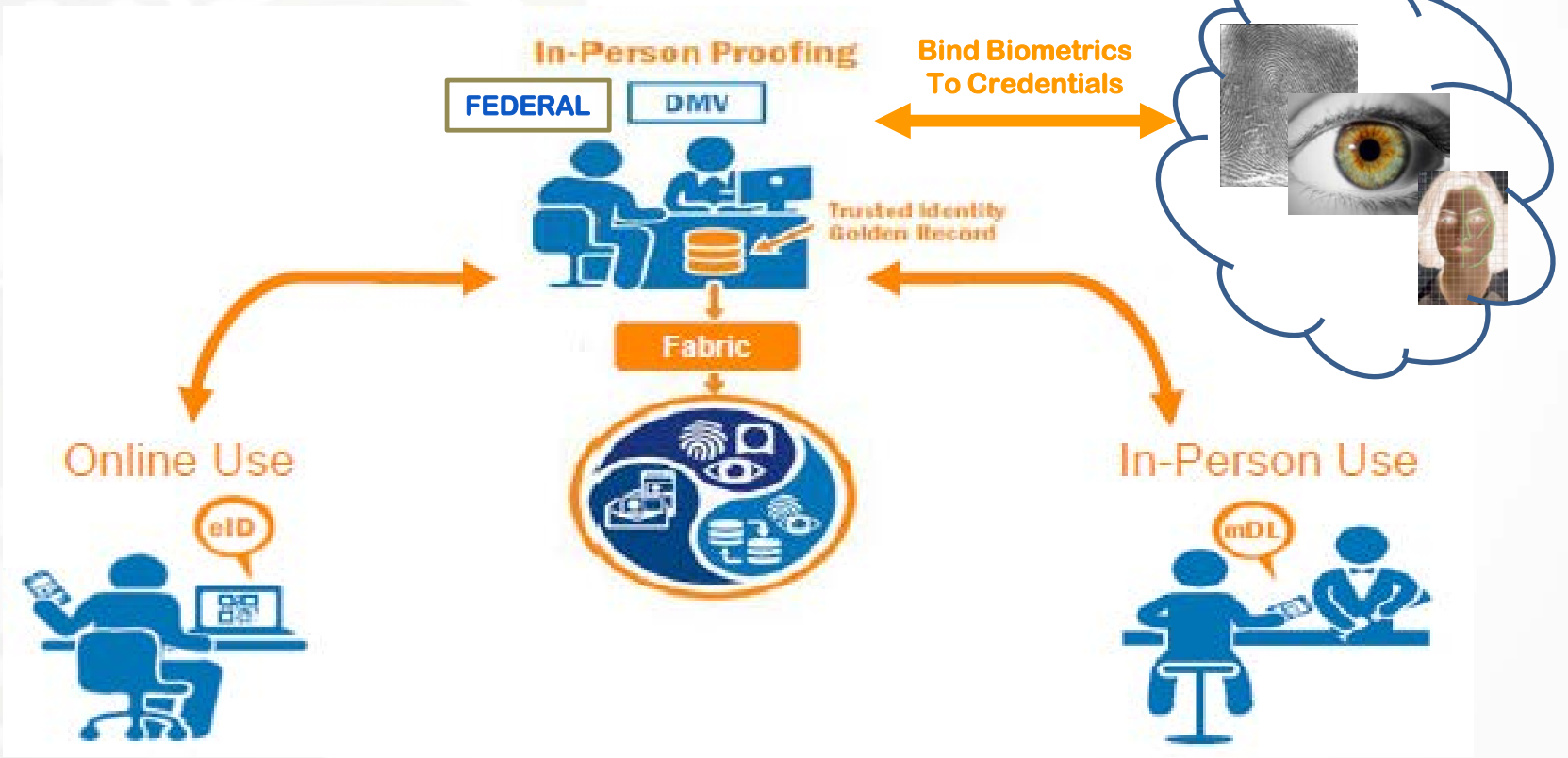
Voice Recognition

DNA

BINDING IDENTITY SO "ONLY YOU CAN BE YOU"

FEDERAL RESERVE BANK of ATLANTA

The enrollment process where the customer's account credentials are initially validated is absolutely critical



BIOMETRICS ACCURACY

FEDERAL RESERVE BANK of ATLANTA

- Key difference with biometrics against other electronic authentication methods—the presence of the “gray” area
  - Password/KBA match is either “Yes” or “No”
  - Since biometrics uses an algorithm to derive a calculated value, there is rarely a complete match between the value of the original template and the live template value
    - False negatives – customer dissatisfaction, lost sales
    - False positives – grants impostor access
    - All a matter of level of risk/customer experience impact one is willing to take

TEMPLATES VS. IMAGES

FEDERAL RESERVE BANK of ATLANTA

- Important to recognize difference between biometric capture/storage options
- In most consumer-based biometric systems, *image* of the biometric element is captured and then the key features of the image are extracted and converted through a mathematical algorithm to a *template*
- Result is encrypted for storage for subsequent matching

FINGERPRINTS

FEDERAL RESERVE BANK of ATLANTA

- Oldest biometric modality in usage today
- Fingers have a pattern of ridges and valleys unique to each individual, even twins, known as friction ridges
  - Skin composed of two major layers: inner (dermis) and outer (epidermis)
- Most frequent use was by law enforcement
  - Identify repeat offenders using aliases
  - Background checks for licensing or employment
- Accepted in U.S. courts of law

FACIAL RECOGNITION

FEDERAL RESERVE BANK of ATLANTA

- Most common biometric used by humans to recognize others
  - Incorporated in authentication documents such as passports, driver's licenses and official ID cards
- Benefits of facial recognition
  - High level of consumer acceptance
  - Technology efforts driven by DHS, DOD and LE
- Challenges to facial recognition systems:
  - Facial masks and other alterations
  - Variation in lighting, background and posing angle
- Wide variations among algorithms in demographic performance ranging from undetectable to poor

IRIS RECOGNITION

FEDERAL RESERVE BANK of ATLANTA

- Not the same as retina scan
- Scans vein pattern around the iris (stroma) at the front of the eyeball using near infrared light source
- One of the fastest validation timeframes due to small byte size of template.
- Currently used extensively in military and commercial applications
  - Used in other countries for health care and national identification programs
  - Until recently required separate and expensive capture camera

VOICE RECOGNITION

FEDERAL RESERVE BANK of ATLANTA

- Speaker recognition differs from speech to text in Dragon/MS-Word, etc. voice recognition
- Key challenge is the accuracy due to acoustics, background noise, poor phone connection, microphone quality, and natural variations in same speaker voice
  - Not accepted in U.S. courts under expert testimony guidelines
- As with other biometric modalities, generally coupled with other authentication methods
  - Device fingerprinting
  - Geolocation

BEHAVIORAL BIOMETRICS

FEDERAL RESERVE BANK of ATLANTA

- Behavioral biometrics cover a wide range of certain muscular and skill-based functions
  - 2015 saw the emergence of a form of behavioral biometrics especially with large e-commerce retailers
    - Examines typing speed, key pressure, mouse movement, keyboard shortcuts, page navigation
- Behavioral pattern developed over a series of sessions with the customer that are known to be legitimate
  - Initial fraud attempts can often be detected due to recognized differences between the criminal element and the legitimate customer

PRIVACY CONCERNS

FEDERAL RESERVE BANK of ATLANTA

- While the use of templates should minimize privacy concerns, a significant level of consumer education will be required for any biometric authentication program
  - Geolocation capabilities can create customer concerns about tracking and how the information will be used
- Factors to ease concerns:
  - Transparency
  - Purpose
  - Appropriateness
  - Security

TRUST & CONSENT ISSUES

FEDERAL RESERVE BANK of ATLANTA

- For many (not all) government purposes consent is not relevant – but **notice** is!
  - Most extend some trust to government, but citizens have no realistic options.
- For commercial purposes both consent and trust are essential
- Identity theft is rampant and seems to be getting worse
- Although there has never been a biometric data breach, this distrust definitely extends to biometrics

THE TIMES THEY ARE A CHANGIN’

FEDERAL RESERVE BANK of ATLANTA

Replacing physical credentials & payment

Biometric Boarding
No ID or Ticket

Cashless
Commerce

Mobile Driver
License

Few need all the information on credentials

(*technology will allow us to control what we reveal*)

We Don’t Need All the Pocket Litter!

QUESTIONS & DISCUSSION

FEDERAL RESERVE BANK of ATLANTA

Jim Loudermilk

James.Loudermilk@idemia-nss.com

571-232-3938

Dave Lott

David.lott@atl.frb.org

404-498-7529

JAMES LOUDERMILK

FEDERAL RESERVE BANK of ATLANTA

Jim Loudermilk is Senior Director, Innovation and Customer Solutions, with IDEMIA National Security Solutions, since July 2017. His focus is on applied R&D to advance biometric and other human identification technology. Also, he architects high performance and cost-effective solutions for customer identification challenges.

Previously he was a technology executive with the Federal Bureau of Investigation, 1996 – 2017. He represented the FBI nationally and internationally on identification and innovation issues. He co-chaired the Interagency Biometrics and Identity Forum, and its predecessor the Biometrics and Identity Management Subcommittee of the National Science and Technology Council. He was a member of the FBI Biometric Steering Committee and represented the FBI with the National Science Foundation Center for Identification Technology Research. Actively participated with NSF, IARPA, and DHS in source selections. Provided Director's Office oversight of the $1.2 billion Next Generation Identification (NGI) development, the Consolidated DNA Index System (CODIS) and other major technology developments. He also managed the Science and Technology Branch multibillion-dollar information technology portfolio for 6 years.

Previous FBI assignments included Assistant Director and Deputy Assistant Director for Information Technology Operations, where he was responsible for enterprise systems and applications, computer networks in all three security enclaves, enterprise data centers, four field Information Technology Centers, headquarters and 75 Legal Attaché offices IT support. Directed a staff of over 700 government personnel, and more than 500 resident contractors, with an annual procurement budget in excess of $230 million. He earlier served as FBI Chief IT Architect, Chief IT Strategist, and Deputy Chief Technology Officer.
Earlier still, while Deputy Program Manager, and Chief Engineer, was responsible for design, development, installation, and transition to operations of the Integrated Automated Fingerprint Identification System (IAFIS) representing a $640 million investment to revitalize FBI identification technology. He reorganized the program office to provide direction to a fully integrated, more than 1,000 person, program team with equal government and contractor participation. Received the Attorney General's 2000 Award for Excellence in Information Technology.

Prior to FBI service he held a variety of positions, primarily executive, in private industry developing communications, collection, and analysis systems for the national security community. He was also a soldier.

Jim holds Bachelor's and Master's Degrees in Mathematics from the University of Dayton and the Degree of Applied Scientist in Communications Engineering from The George Washington University. He is also a graduate of the US Army Command and General Staff College.