RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: IDY-T08

FOOL PROOF: PROTECTING DIGITAL IDENTITY IN THE AGE OF THE DATA BREACH

Gregory Crabb

Chief Information Security Officer & Vice President
United States Postal Service
@USPS

Paul Grassi

Partner & SVP of Cybersecurity
Easy Dynamics Corp
@pgrassi

Identity Management: The Issue

A common culprit of data breaches is ***poor digital identity and access management***. Hackers use stolen identity credentials to ***gain access to privileged data and applications.***

Challenges to Digital Identity Management

1 Demographics Matter

- A single proofing process ***does not exist*** to successfully proof the range of demographics attempting to access a digital service
- The same is true of authentication – ***what works for one product may not work for another***
- Market solutions ***primarily work for the wealthy***

2 Distributed Applications

- Organizations rely on an ***increasing number of applications*** to conduct business
- Organizations must create a ***singular user identity*** that confers access to applications without compromising network security

3 Access Provisioning & Deactivation

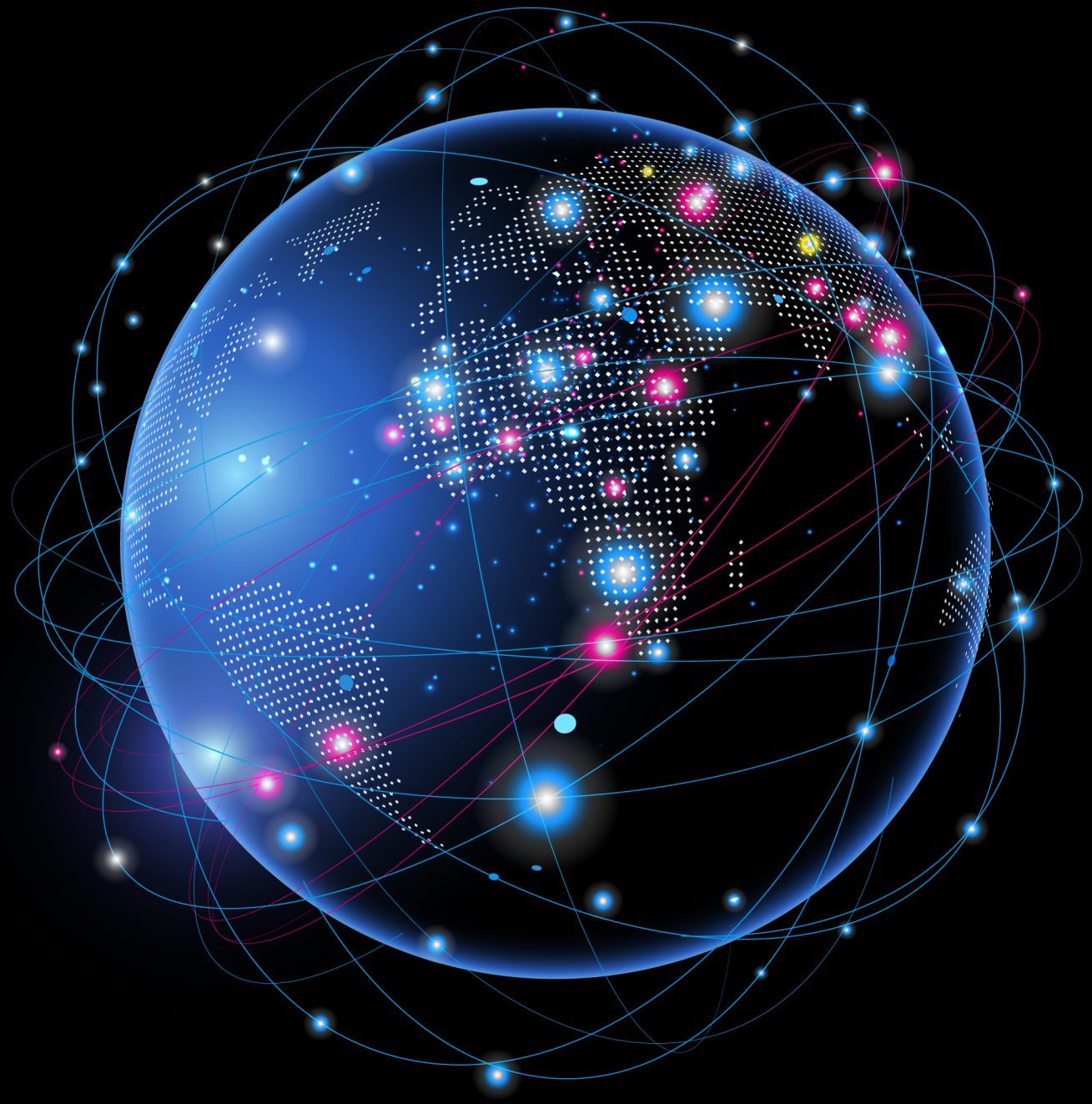
- Employees join, leave, and move throughout an organization at an ***increasing rate***
- Organizations must develop a ***consistent mechanism*** for ensuring an employee's access level is up to date and commensurate with their role requirements

4 Security vs. Usability

- Traditional knowledge based authentication (KBA) methods ***do not always provide sufficient protection***
- Organizations must develop ***enhanced identity verification capabilities*** to ensure the validity of a user's digital identity

The average cost of a major data breach to a U.S. business between 2016 and 2017 was **$7.35 million** and is trending up.

Remote, scalable attacks are simple in today's proofing paradigm



Identity Proofing: First Line of Defense

Through the use of sophisticated identity proofing processes, government agencies can ***ensure the integrity of sensitive data and combat cyber criminals.***

Identity Proofing Process

1 *Resolution*

Resolve a claimed identity to a single, unique identity within the context of the population of users

2 *Validation*

Validate that all supplied evidence is not counterfeit

3 *Verification*

Verify that the person you are transacting with ***holds the claimed identity***

Leveraging Identity Proofing as the First Line of Defense to Maximize Network and Custom Data Protection

Benefits of Identity Proofing include:

- Mitigating fraud
- Reducing improper payments
- Improving service delivery and customer service by saving personnel from having to review fraudulent applications
- Addressing employees' and customers' concerns for privacy and identity protection

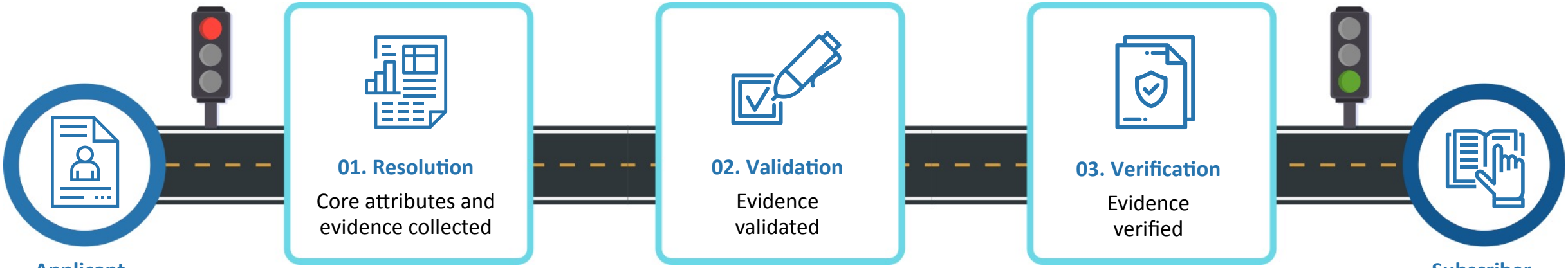
Identity theft is ***the fastest-growing crime in the U.S***. There was a 44% increase in identity-related breaches from 2016 to 2017.

POLL QUESTION 1

IS IDENTITY PROOFING PART OF YOUR ORGANIZATION'S FRAUD REDUCTION STRATEGY?

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3815

A “Framework for Proofing”



Individual uniquely distinguished among a given population or context

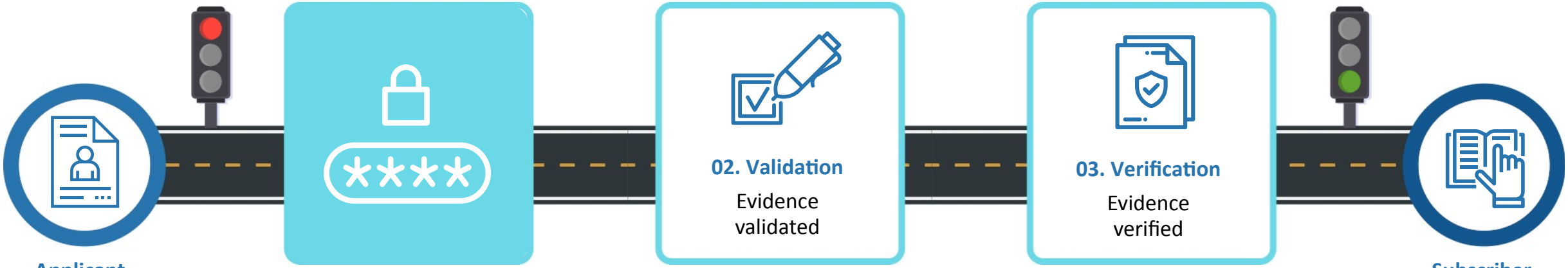
Authenticity, validity, and accuracy of identity information determined and related to a real-life subject

Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established

PROOFING IS JUST THE FIRST AUTHENTICATION

Identity proofing should be comparably secure to the traditional authentication process (based on risk)

A “Framework for Proofing” – Step 1



Individual uniquely distinguished among a given population or context

Authenticity, validity, and accuracy of identity information determined and related to a real-life subject

Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established

WHAT YOU KNOW

A “Framework for Proofing” – Step 2

Individual uniquely distinguished among a given population or context

Authenticity, validity, and accuracy of identity information determined and related to a real-life subject

Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established

WHAT YOU DO

A “Framework for Proofing” – Step 3

Individual uniquely distinguished among a given population or context

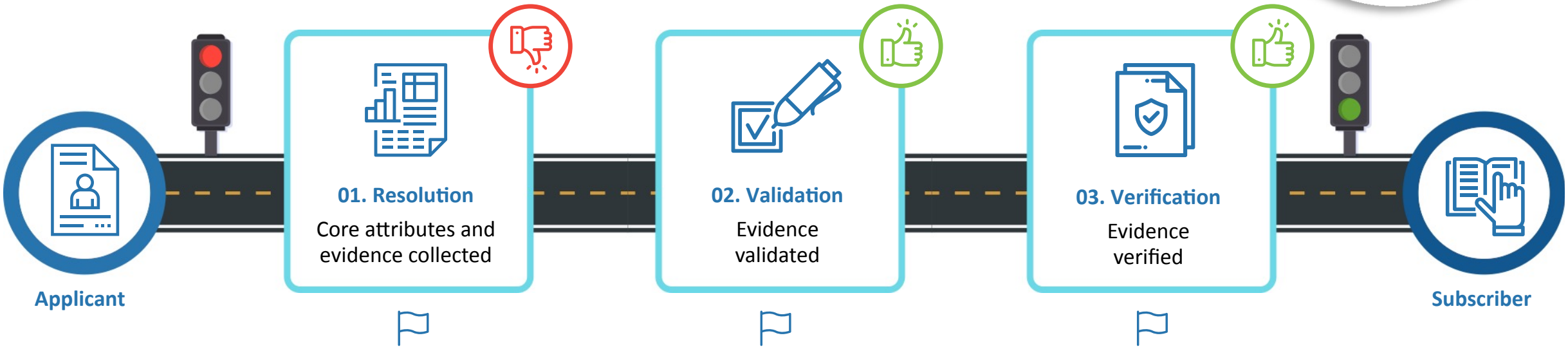
Authenticity, validity, and accuracy of identity information determined and related to a real-life subject

Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established

WHAT YOU ARE

Can we drive the street value of our data down to 0?

A “Framework for Proofing” – The Result



Individual uniquely distinguished among a given population or context

Authenticity, validity, and accuracy of identity information determined and related to a real-life subject

Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established

Remote, Scalable: Tough
Targeted, Unscalable: Tough

Evolving Identity Proofing Capabilities

Identity authentication (authN) solutions confirm a user's digital identity based on their ***ability to provide established credentials***.

Next Generation Identity Proofing Concepts

Increasing Complexity

Dynamic Knowledge Based Authentication (KBA)

Validate ownership of existing digital assets leveraging frequently changed information

Derived Trust

Proof of possession of an authenticator bound to a high assurance identity

Analytics

Networks and devices track user behaviors to define standard profiles. Privacy and binding characteristics are key

Social/Web of Trust

As another coordinate, combine social data, web of trust, analytics, and other information to identify an individual

While organizations have historically relied on KBA to authenticate identities, multiple ***coordinates of identity evidence and activity can increase confidence in identity.***

A Note on the Technology that Shall Not Be Named

Just because it is immutable, or even signed, does not mean it is right

What is the U.S. Postal Service doing?

Our identity and access management (IAM) solutions serve as the front door for the entire Postal Service enterprise – supporting over 600,000 users and 900 distinct applications. As part of our IAM strategy, we are always working to ***implement identity proofing and control enhancements.***

Identity and Access Management Strategy

The Postal Service plans to achieve more precise identity access control thorough advanced identity proofing and management solutions, integrating foundational IAM capabilities with next generation technology:

- User and Entity Behavior Analytics
- Automation & Orchestration
- Adaptive Privilege Management
- Identity Convergence

Additionally, the Postal Service is developing innovative **Identity Verification Services (IVS)** and **Identity Shared Services (ISS)** to improve internal personnel functions and generate revenue.

Identity Verification Services (IVS)

- **Enhancing identity verification services** to reduce USPS onboarding costs and improve the quality, speed, and security of HR processes
- **Expanding our portfolio of biometric capture** capabilities available to partnering federal agencies

Identity Shared Services (ISS)

- **Leveraging IVS and IAM capabilities** to provide revenue generating products to USPS customers
- **Providing identity-based verification**, federation, and transaction validation services

Identity Proofing Use Cases

The rapid expansion in identity proofing technology has created ***a range of possible use cases.***

Industry Use Cases for Identity Proofing

- **Facility and Physical Security**
- **Transportation Security**
- **Finance**
- **Computer Security & Anti-phishing**
- **Talent Management**
- **Government Services**

Identity Proofing at the Postal Service

The Postal Service is committed to identifying and delivering innovative solutions for the **creation, verification, and management of secure identities** to best protect its network, customer, employee, and business partner data.

Identity Proofing in the Government & Private Sector

As identity proofing technology continues to improve, government agencies and private sector companies will be able to utilize identity proofing solutions to ***fulfill market needs across a range of industries.***

Industry Use Cases for Identity Proofing: Government Sector

Computer Security & Anti-phishing

Track keystroke patterns to validate the identity of individuals sending emails and identify potential phishing attempts

Transportation Security

Apply biometrics scanning devices (iris scans, fingerprint readers) to bar unauthorized individuals from accessing a vehicle

Government Services

Perform **virtual identity proofing,** allowing real-time biometric attributes captured over video to be compared to photo IDs

Industry Use Cases for Identity Proofing: Private Sector

Facility and Physical Security

Use facial recognition and advanced video monitoring to detect unauthorized entrants to a facility

Talent Management

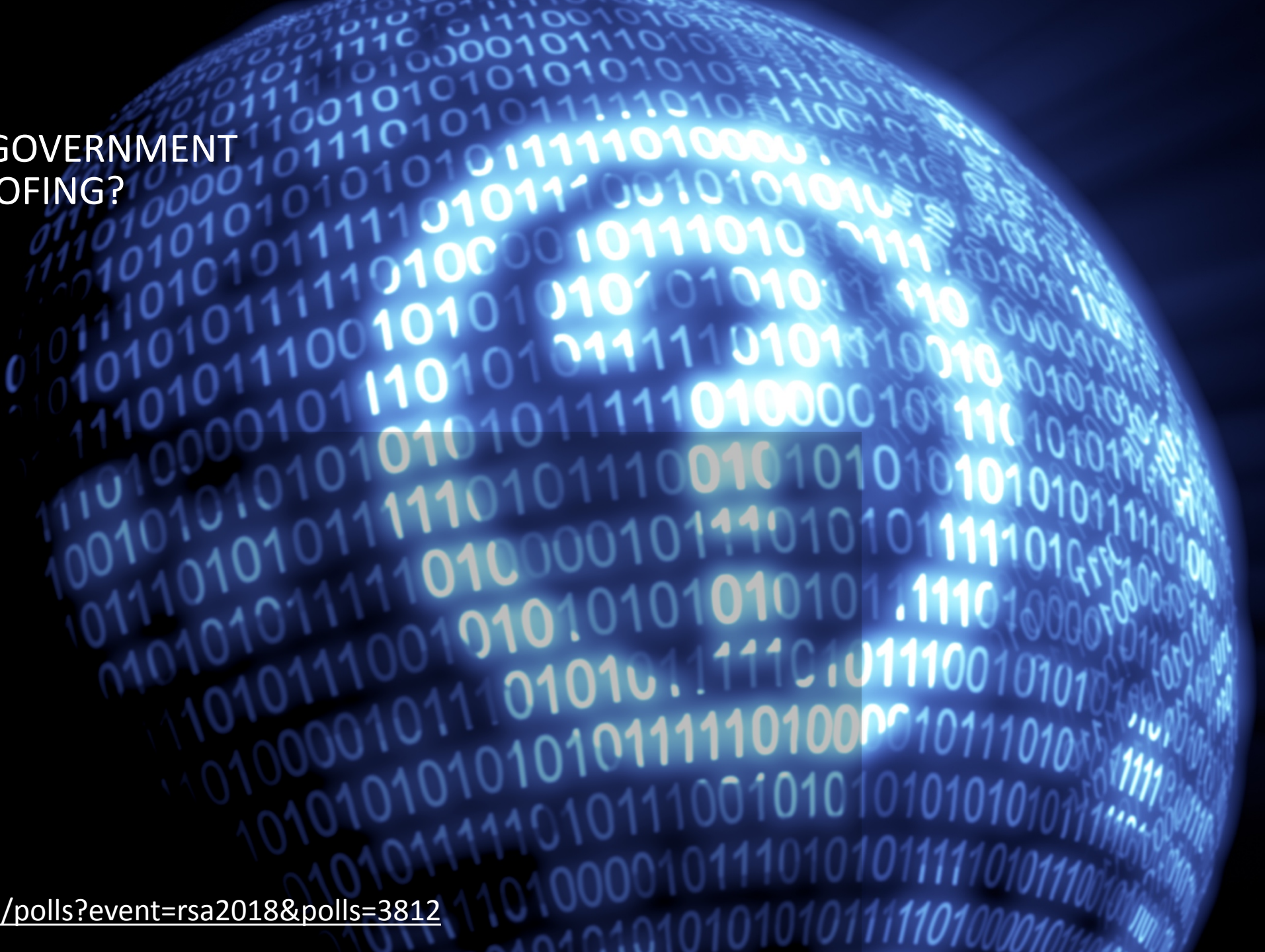
Require employees to validate time and attendance data by providing biometric identifiers (iris scans, fingerprints)

Finance

Request individuals provide biometric identifiers (iris scans, fingerprints) to **prevent fraud in online financial transactions**

Poll Question 2

WHAT ROLE SHOULD GOVERNMENT PLAY IN IDENTITY PROOFING?



https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3812

Path Forward for Identity Management

Organizations should pursue several ***immediate and long-term actions*** to modernize identity proofing and improve overall cybersecurity resilience.

Short-term

Optimize Enterprise-wide Authorization Standards

- Employ facial recognition technologies, high resolution scanning, and biometric detection **to confirm the identities of network users**
- **Source modern identity proofing technologies from solution providers** to bridge the gap between traditional KBA techniques and modern methods

Mid-term

Develop Continuous Authentication Capabilities

- **Continue to develop advanced identity monitoring tools** that allow for consistent observation of various identity attributes: typing rhythm, mouse patterns, iris patterns, etc.
- Refine strategies for **leveraging each customer interaction** as an opportunity to collect identity related data to prevent fraud and improve customer service

Long-term

Explore Disruptive IAM Technology

- **Leverage the adoption of analytics and smartphone technology** to create new, highly secure identification documents
- Continue to **explore identity proofing technology** that enhances the identity convergence between the physical and digital worlds

Applying Identity Proofing Technology in your Organization

To successfully ***apply*** identity proofing technologies, your organization must first ***understand*** the challenges and opportunities associated with identity proofing solutions and ***embrace*** the changes to normal work processes that accompany new technology implementations.

Key Considerations

Educate	Learn	Apply
• What are the **cultural and technical challenges** associated with implementing identity proofing technology? • Which solutions match my organization's **unique needs and demographics?**	• How can I convince my workforce that "what you know" (KBA) is **not a sufficient** identity proofing mechanism? • How do we vary and customize our identity proofing requirements to **avoid a "once-size-fits-all" approach?**	• How do we evolve our identity proofing standards to **eliminate KBA mechanisms?** • How do we position ourselves to **grow our identity proofing practices** without buying in to every new trend?

Timeline for Applying Identity Proofing Technology

Organizations should take actions in the ***short, medium, and long term*** to apply identity proofing technology.

Weeks

- Understand your organization's **demographics**
- Define a **long-term organizational strategy** for identity proofing

Months

- Begin to **phase-out KBA mechanisms**
- Explore and evaluate an **identity proofing solution**

Years

- **Expand demographic coverage** for identity proofing solutions
- Monitor and **evolve existing solutions**
- Define **account recovery** capabilities

Poll Question 3

WHAT PROCESS OFFERS THE HIGHEST LEVEL OF CONFIDENCE IN PROOFING A REMOTE IDENTITY?

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3813

In Summary

Modernizing ***digital identity and access management capabilities*** to strengthen cyber resilience needs to be a priority of every organization.

Iterate challenges associated with identity and access management

Develop solutions to enhance identity proofing capabilities

Expand demographic coverage

Develop analog methods as an Identity Management solution