RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **IDY-RO1**

# Operationalizing Identity: IAM for Customer Service

**Arynn Crow**

Manager of Product Management, User Authentication
AWS
Twitter: @arynncrow

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

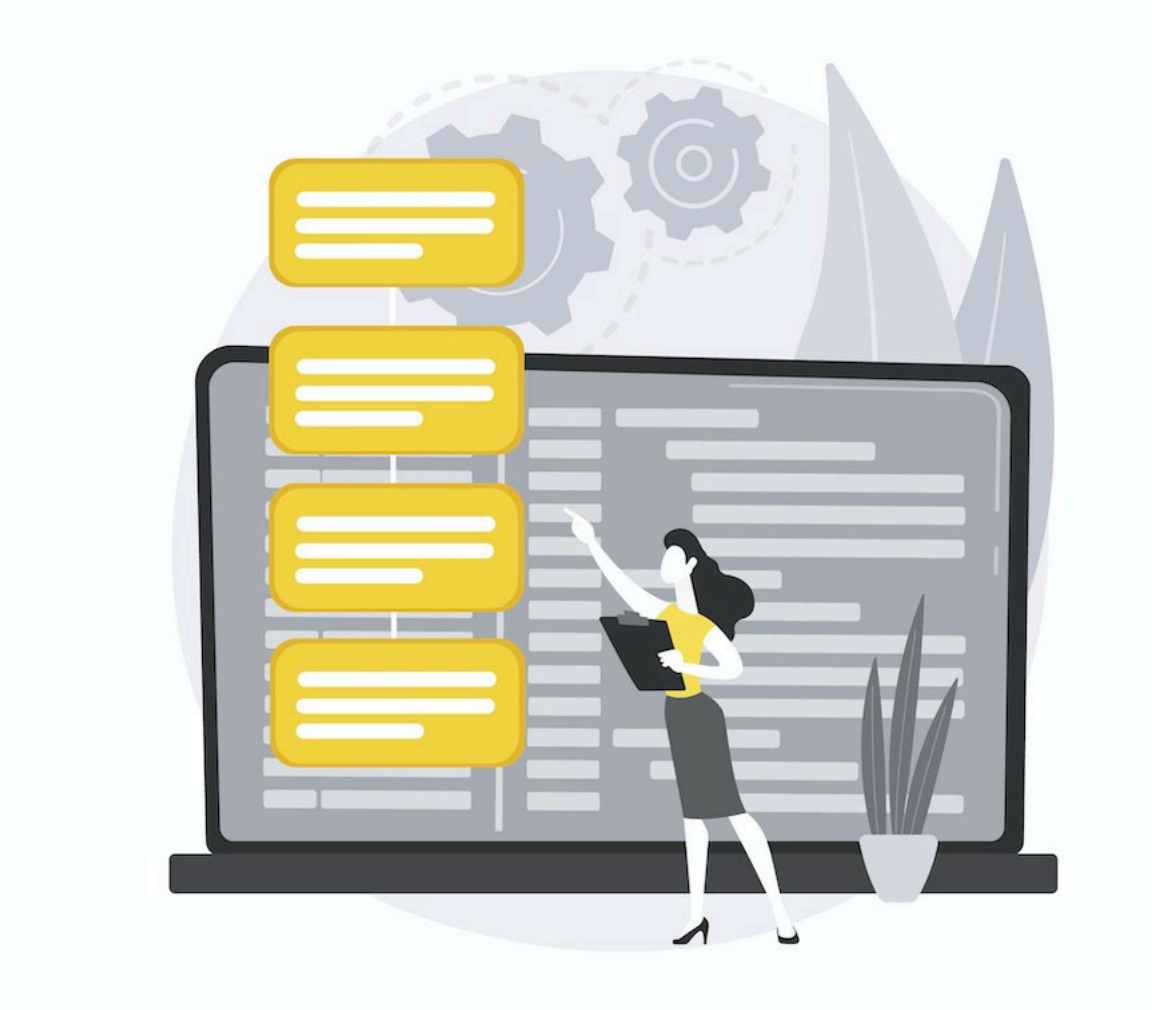
# Welcome!

# So, what are we doing here?

We'll cover…

- Common use cases and risks
- Customer versus workforce considerations
- How to distill these considerations into a plan

# I. Use Cases and Risks



# The Customer Service Landscape

- Customer service is anywhere your customer is interfacing with your organization
- Customers have high expectations, and agents have advanced capabilities to meet those expectations
- High expectations, but communication  channels are limiting

# Common Use Cases

- Seemingly innocuous and transactional – where's my order, replacements
- Help with compliance and data requests
- Configuration help for user or business accounts
- Modifying critical account information – including, when self-service fails, account recovery

# Many Use Cases, More Data Access

- Access to PII, such as…
- Payment and billing data
- Social security numbers, birth dates
- Personal documents – utility bills, driver's licenses, bank statements, etc.

# Agents May Have Advanced Privileges

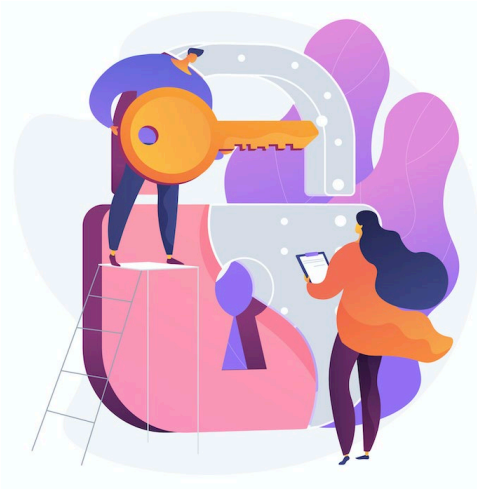
- Add, change, remove payment & billing information

- Modify user credentials

- Change account state or suspend account/ service

- Place orders, take other actions on customer's behalf

# Your objectives are…



## Prevent Account Takeover and Fraud

- Humans are biased to empathy
- Social engineering is increasingly common
- Customer service is the most visible human interface

## Prevent Data Exposure

- Monitor and minimize internal and external access
- Customers in different demographics can have different data sensitivities

# II. Considerations for Customers and Workforces


Customers

Workforce

# Authentication

- Agents determine that customers are who they say they are – this is the primary or only defense for many organizations
- Familiar authentication challenges are complicated by channel –sign-in portal protections may be unavailable
- Customers expect help from anywhere any time. This creates tension between security and satisfaction

# Authentication Methods - Continued

**Knowledge-Based Authentication (KBA)** – weak, but persists due to ease of use

# Authentication Methods - Continued

- **PINs and Passphrases** – May or may not be specific to customer service.
- Customers reuse these, and internal/external actors may replay them

**PIN**

- 931234

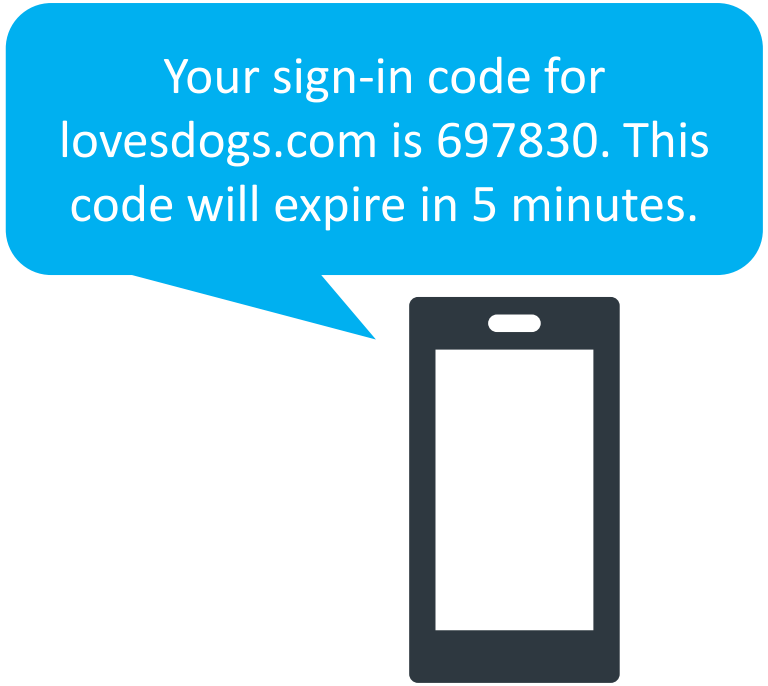
**Passphrase**

- ilovemydog2022

# Authentication Methods - Continued

- **SMS and email OTP** – Persists due to ease and wide availability.

  (May provide incremental assurance over KBA)

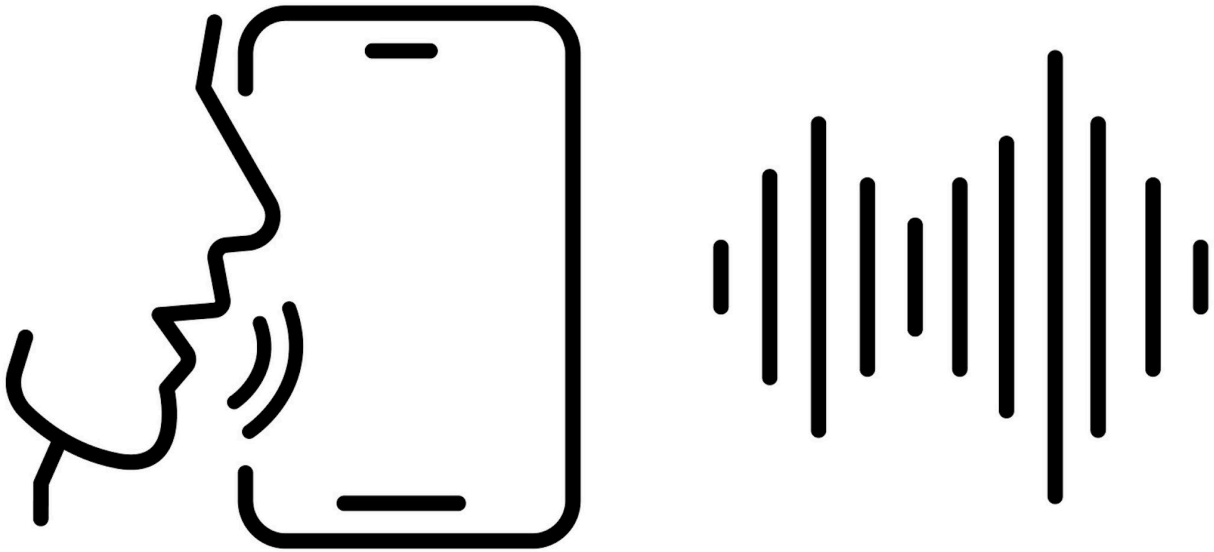


# Authentication Methods - Continued

- **Push notifications** – Easy to use. May also benefit stronger sign-in protections from a mobile app

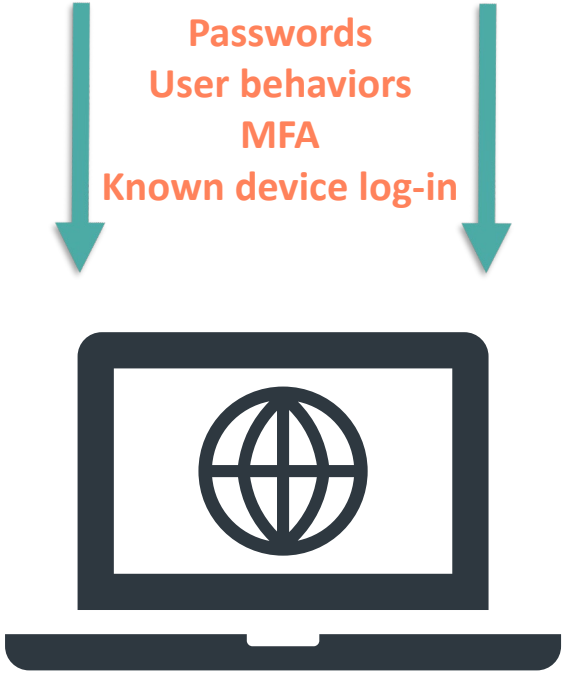
# Authentication Methods - Continued

- **Voice Biometrics** – easy, relatively high assurance, fast and low-friction
- Privacy and implementation caveats

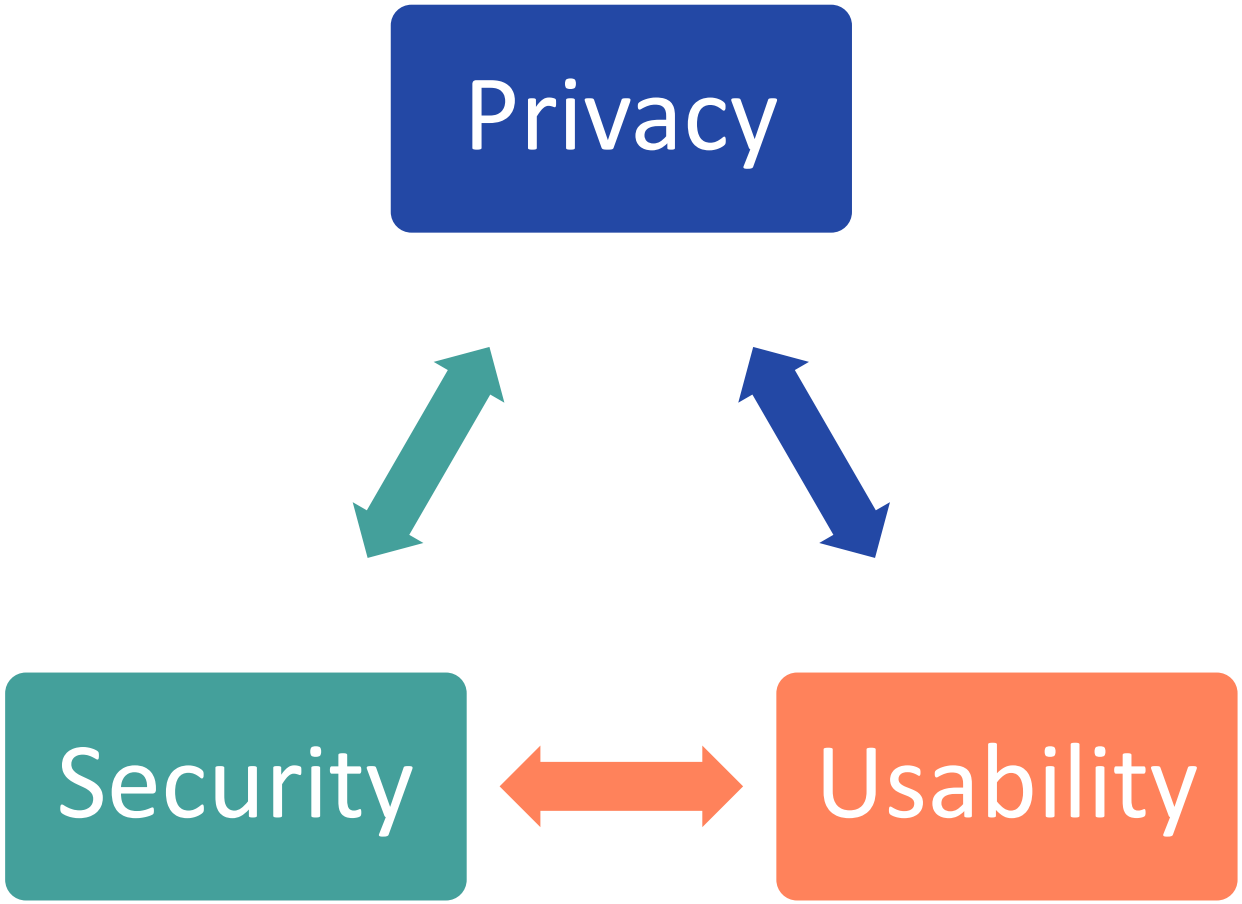


# Authentication Methods - Continued

- **Browser sign-in** – Limited use cases, but benefits from full controls of your authentication stack. Won't work for recovery!

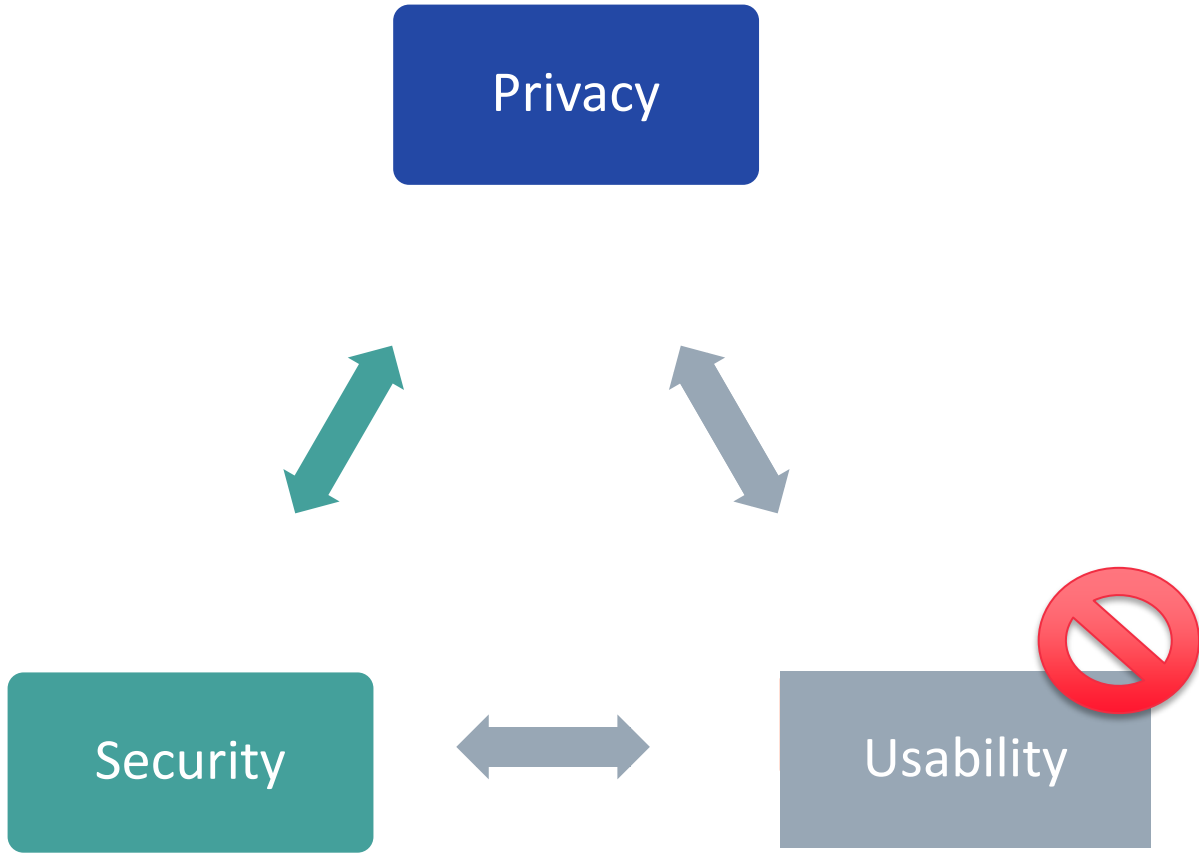


# Deciding what to apply



# Use Force Only as Necessary

- Using the toughest controls in all scenarios may marginally improve posture
- …but it will will also frustrate your operations teams and customers
- Agents are the closest to our customers of any staff



# Assurance Levels Apply

- Authentication assurance – step up authentication applies to customer service, too
- Lower-assurance challenges may be acceptable for lower-risk operations
- Higher-assurance challenges for higher-risk operations

# Automation

- Automating low-level requests reduces costs and risks of manual work
- Automating sensitive functions like account recovery could introduce new risks
- Use automation and dynamic controls to augment processes that require human review

# Your Workforce

# Multi-Factor Authentication

- Users may not have access to USB ports or mobile phones
- OTP tokens are still common in physically constrained environments
- NFC, Bluetooth, etc. may occasionally be used

# Authorization and Access

- Access control can be complicated by unique data sources and high degrees of change, ambiguity in work
- Customer service access requirements are often seasonal/fluid, challenging modern attribute-based access methods
- Overlapping job functions; separation of duties may be poor
- Especially important for RBAC models and organizations with loose hierarchies

# More Complexity - Contractors

- Contractors may not use the same practices, technologies, standards for identity management
- Consider technical interoperability as a requirement, not an implementation detail while selecting vendors

# Putting It All Together

# Map the Current State

- Get to know your customer service stakeholders (agents, management)
- Learn what metrics, KPIs, and current state concerns (call handling time, customer satisfaction)
- Lean on **both** security and operations SMEs to build a threat model

# Build a Risk Management Framework



**Probability**
Rare - 1
Unlikely - 2
Moderate - 3
Likely – 4
Almost Certain - 5

**Impact**
Minimal – 1
Low - 2
Medium - 3
High - 4
Severe - 5

| Risk | Likelihood | Impact | Score | Control |
|---|---|---|---|---|
| **PIN replay** | **2** | **5** | **10** | **Automated entry** |
| **Unauthorized purchase** | **3** | **4** | **12** | **SMS confirmation** |

# Considerations for Change Management

- Customer service is downstream; change is difficult and not fully within their control
- Understand how changes impact the employees – vet solutions with your frontline staff
- When solutions cause churn, people work around them