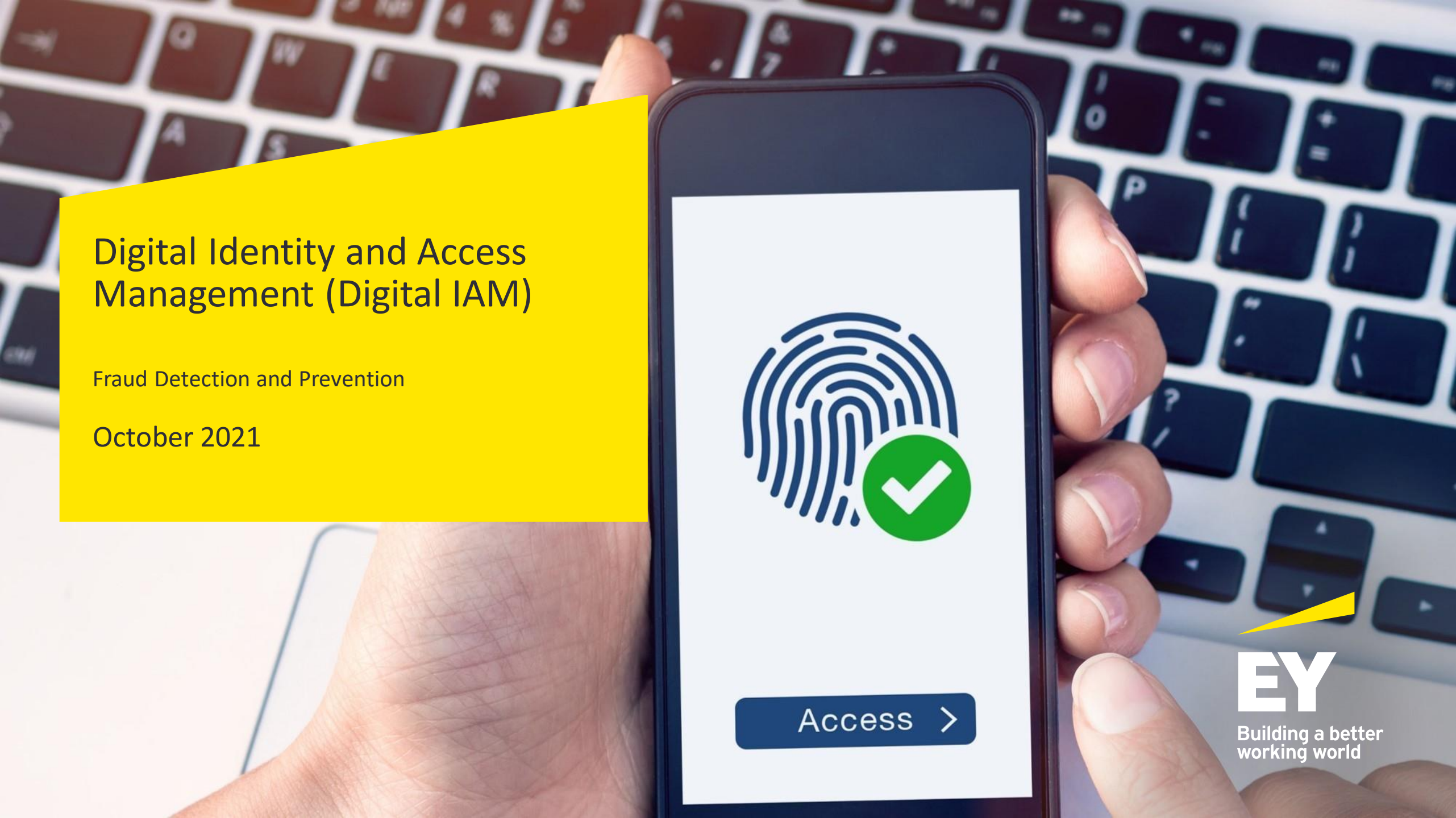
Digital Identity and Access Management (Digital IAM)

Fraud Detection and Prevention

October 2021



Building a better working world

Here with you today



Rob Foster

Solution Architect
Customer IAM and Fraud Prevention
Cyber Security



Sharmila Gupta

Solution Architect
Customer IAM and Threat Management
Cyber Security

OBJECTIVES

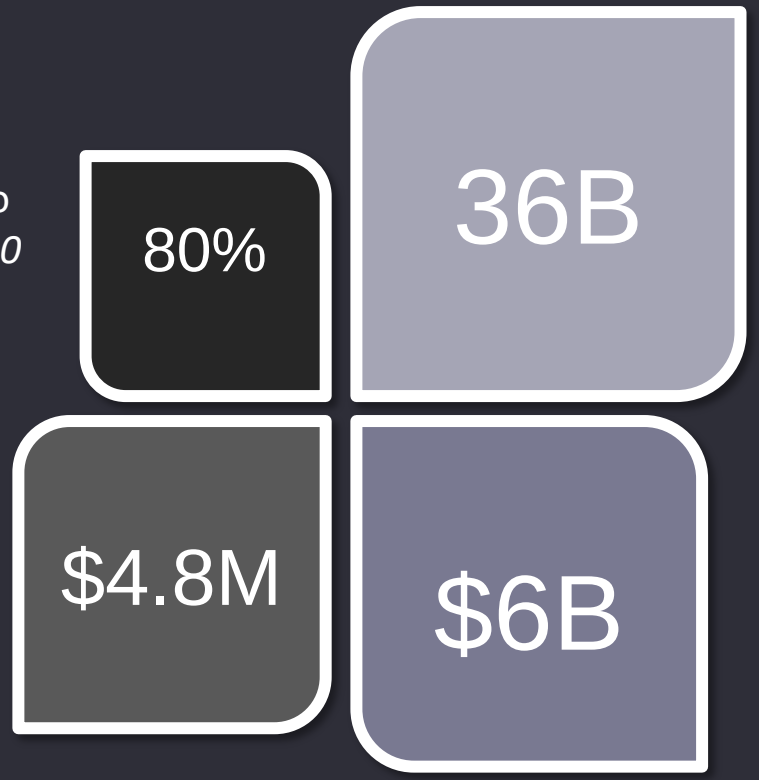
1. Understand Identity and Access Management
2. Understand key trends and challenges with customers
3. How to address fraud detection and prevention with Risk Assessment and ID Proofing
4. Understand De-centralized ID and how it enables a globally trusted ecosystem

Overview



Digital identity trends & challenges

Hacking-related breaches are linked to compromised passwords *[Verizon 2020 Data Breach Investigations]*



Records exposed because of data breaches in first half of 2020 *[RiskBased]*

Identity theft and fraud reports in 2020, up 45% since 2019 *[Federal Trade Commission]*

Loss annually by Banks due to Synthetic Identity Fraud *[Forbes]*

Reputational risk

Financial loss

Tax & Insurance Fraud

Identity Theft

Government benefit fraud

What do identities look like today

Human

- **External users: B2C consumer**
- **External users & admins: B2B customers**
- **External users & admins: Vendors & Providers of products and services**
- **External users: Contractors**
- **Workforce users & admins: Corporate employees, store employees, distribution center & warehouse employees, affiliates**



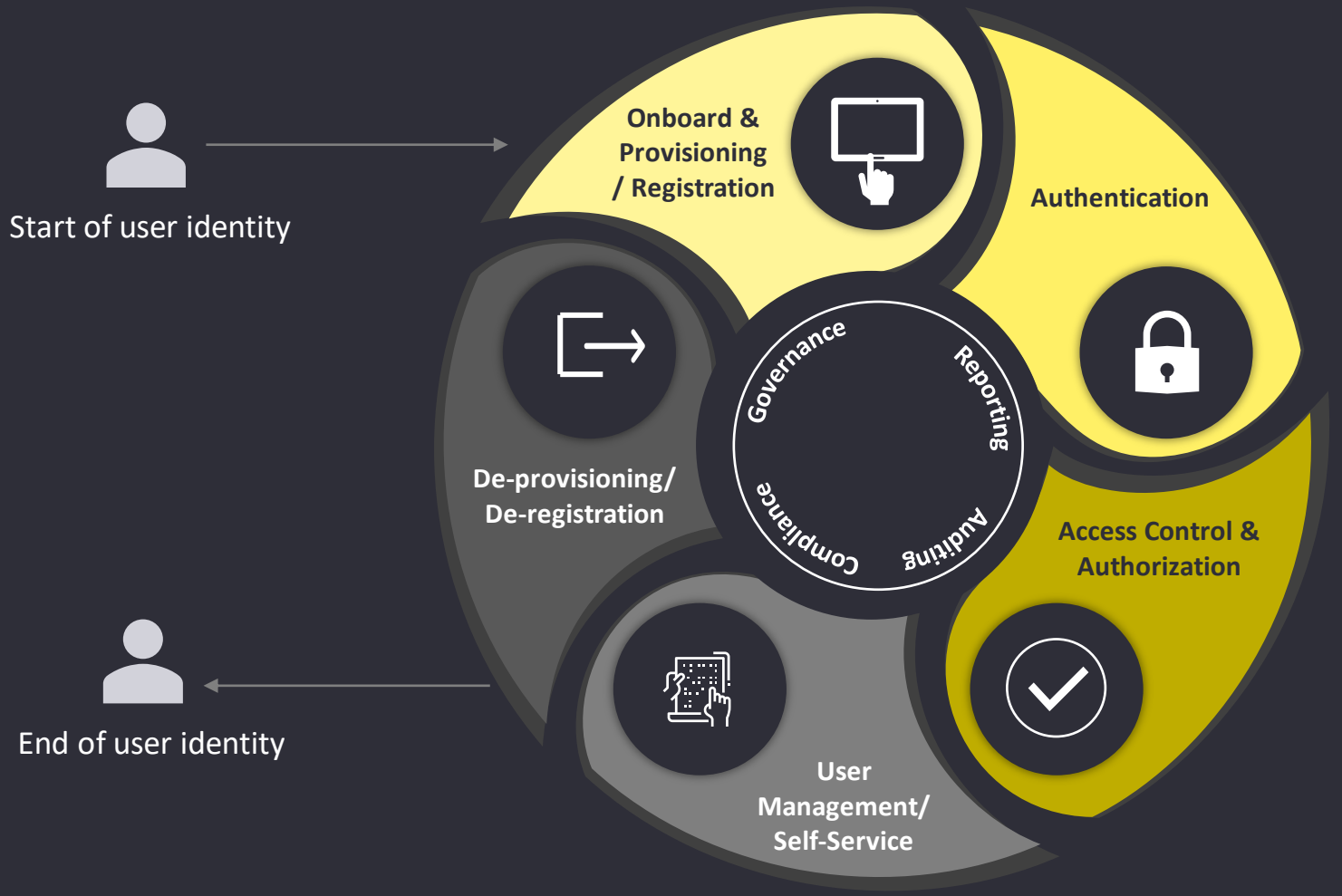


Non-human

- **Devices: Mobile phones, laptops, tablets, smartwatch, Intelligent assistant devices (IA)**
- **IoT sensors: RTLS (WiFi, Bluetooth, LE, UWB, RFID), environmental sensors**
- **Other IoTs: Biometric scanners, cameras, bots, tools & appliances**
- **Machine oriented: Service accounts (internal, external & cloud), service APIs**

Identity & Access Management

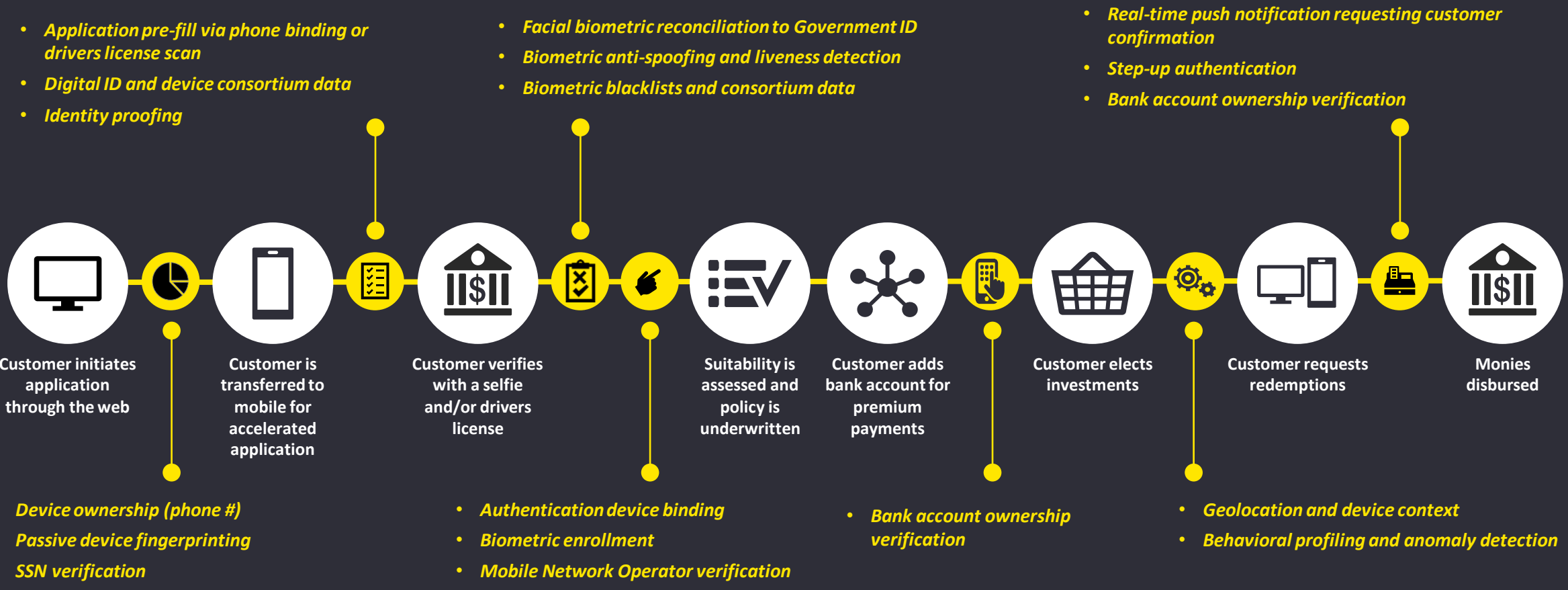
User identity Lifecycle



Leading practices

Fraud can take place across all stages of the customer life cycle … identifying the risks and mitigating controls is critical

Digitization has shifted the identity, authentication, and fraud management paradigm and risk evaluation must be performed continuously throughout the customer lifecycle. A sample of the multitude of identity, authentication, and other supporting capabilities that could be invoked across an insurance product are illustrated below:



Industry challenges in addressing synthetic identity fraud

Synthetic identity fraud is the fastest growing financial crime in the US for several key reasons:

Lack of consumer victim

Synthetic identity fraud has no consumer victim to raise a red flag, as financial institutions take the loss. As a result, the fraud stops only when the fraudster conducts a credit bust-out.

Difficult to Differentiate

Synthetic identity fraud is typically charged off as a credit loss. Many firms cannot systematically identify these types of fraud, even after the fact, unless an investigation is manually triggered.

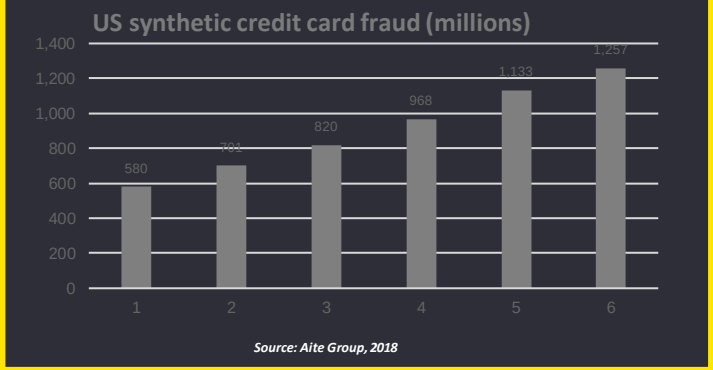
Weaknesses in Identity Controls

Fraudsters increasingly use complex patterns exploiting data breaches and weaknesses in underwriting to attack customer identities. Current fraud solutions struggle to prevent identity-related losses.

Driven by Digital Volumes

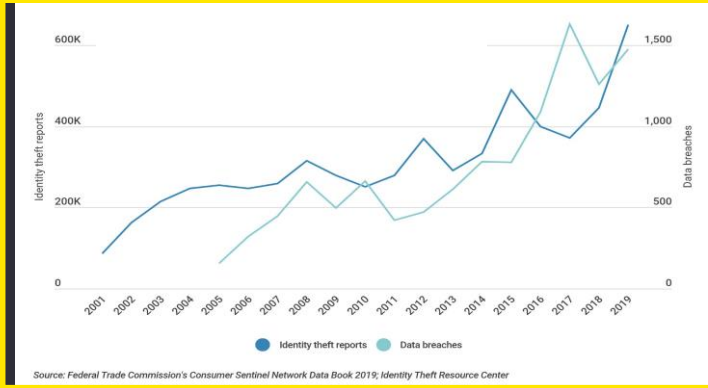
Synthetic identity fraud preys on digital interactions and online transactions. COVID-19 related increases in digital volumes are driving higher synthetic identity fraud risks.

Synthetic identity losses continue to grow year-over-year



Source: Aite Group, 2018

Data breaches continue to increase, with over 6.2 billion records exposed in the past 5 years



Source: Federal Trade Commission's Consumer Sentinel Network Data Book 2019; Identity Theft Resource Center

Increase in data breaches increases the amount of fraud losses as a result of stolen identities



30-40% of 2020 fraud losses will be related to online transactions



25%+ of 2021 US consumer credit charge-offs will be driven by first-party fraud according to Experian.

Digital IAM Capabilities to address identity fraud



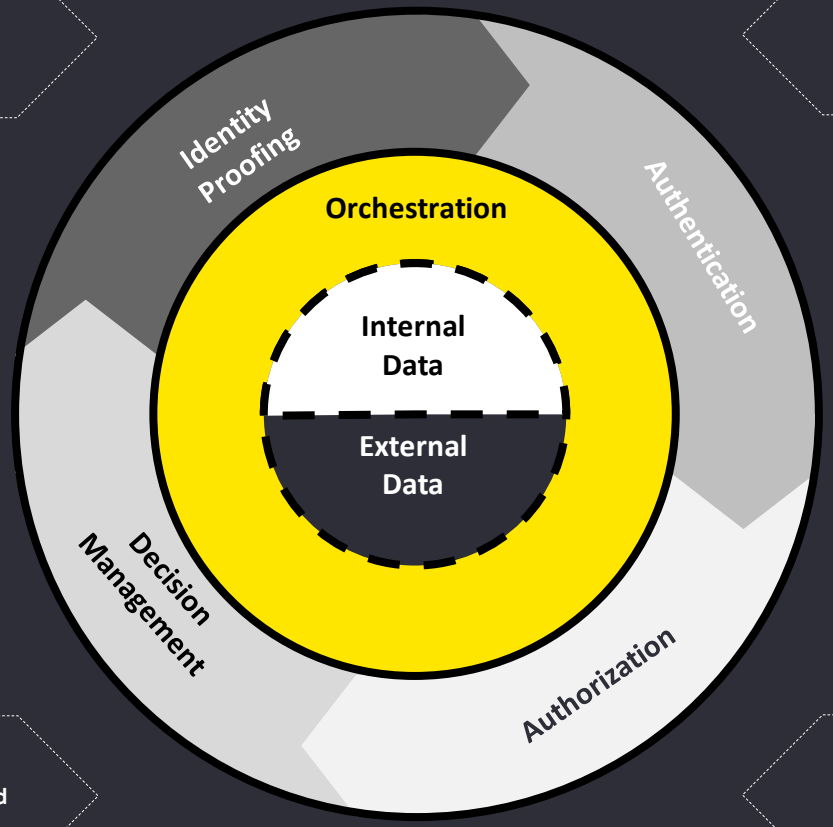
Leading practices

What are the components of a leading identity ecosystem?

Customer identity is about more than just authentication. The customer identity lifecycle starts from the creation of the identity and associated identity proofing (e.g. new account opening), through the enrollment of authenticating factors and subsequent authentication, through authorization, and decision management. This continuous feedback loop is further supported by internal and external identity data and orchestration.

Identity proofing encompasses the creation of new identities within the enterprise as well as the verification that asserted identity attributes are actually connected to the identity.

1. Creation of identity
2. Identity verification
3. Digital and device identity binding



Authentication allows individuals to present different knowledge, possession, and/or biometric factors to verify they are who they claim to be.

1. Enrollment
2. Active Authentication
3. Passive Authentication

1. Risk-based authentication
2. Behavioral biometrics
3. Device and channel-based intelligence

Decision management supports the enterprise in determining when customers should be challenged with authentication and what factors should be offered.

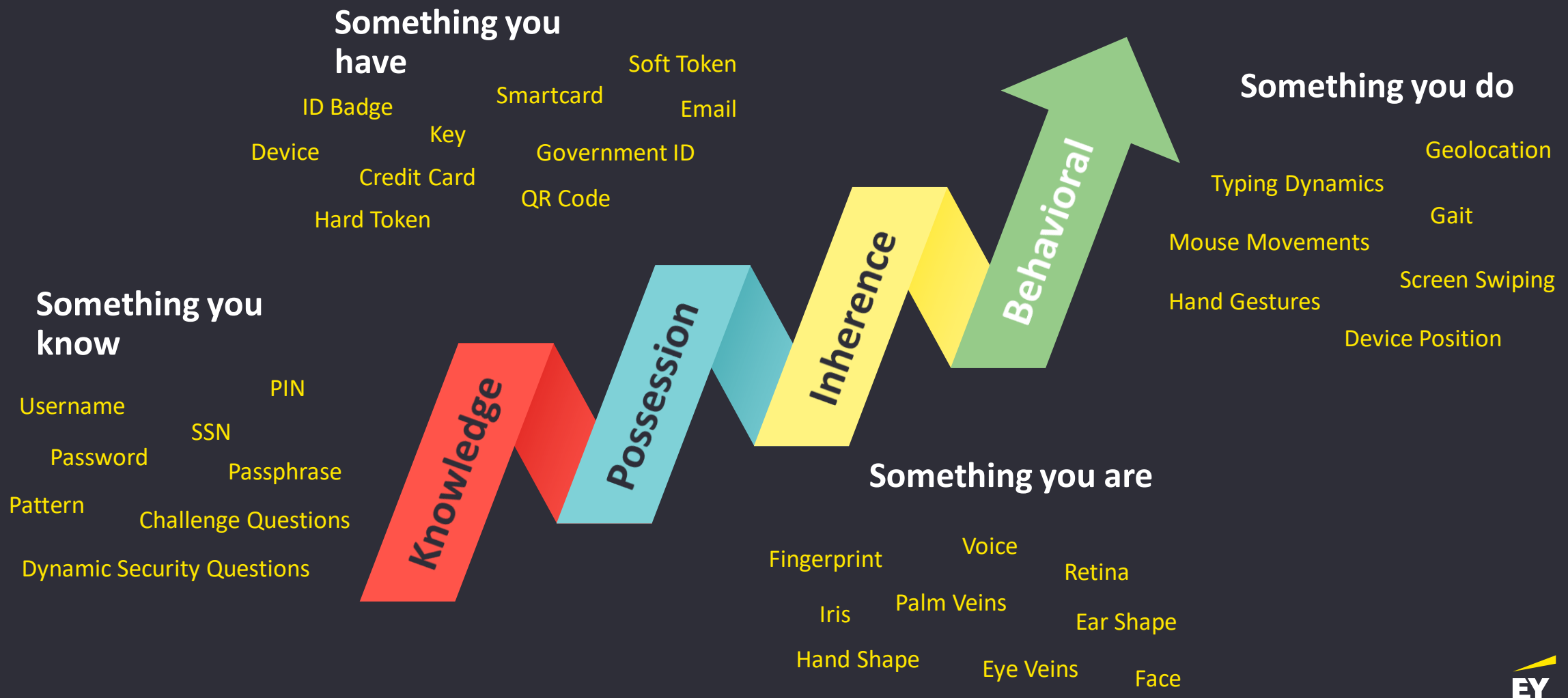
1. Access Control
2. Transaction Verification
3. Third-party Access

Authorization defines what an identity is permitted to access and what activities can be performed.

Leading practices

What authenticators exist to help mitigate fraud risk?

There are four modalities of authentication. Each modality has inherent strengths and weaknesses across a number of dimensions including security strength, spoof-ability, breach history, invasiveness and others. Selecting and offering the appropriate authenticators should balance the desire for security and the impact to the user experience.



Identity cannot be on an island — integration with fraud, cyber, and digital is imperative given the rapid pace of digitization…

Identity, fraud, cyber, and digital convergence delivers many benefits, including:

Faster time to market

Collaboration between identity, cyber, fraud, and digital will enable rapid development and deployment of new products, channels, and interaction capabilities, all whilst balancing customer experience, security, and risk

Reduction in cost to serve

Digital enablement will shift customers from high cost-to -serve channels like call centers and paper to web, mobile, and IoT self-service capabilities

Customer-centric experiences

Consistent and risk-balanced omni-channel customer experience will drive share-of-wallet and customer stickiness

Reduction in fraud losses

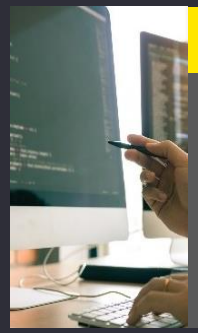
Holistic real-time, data-driven and integrated fraud and cyber decisioning will serve to reduce fraud while optimizing customer “friction”



De-centralized ID



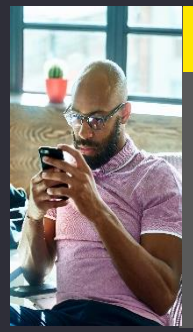
The way we manage identities today is problematic



Security vs. Usability: User experience (UX) has measurable business impact

The traditional ways we collect and manage customers' data and manage their accounts tend to be lengthy and complicated, and can interrupt the flow of business.

The impact: businesses stand to lose customers and retail opportunities due to drop outs during these processes.



Privacy matters, and users are increasingly protective of it

Customers and business partners are increasingly aware of the tradeoff between privacy and convenience. The balance is shifting in favor of protecting their data.

The impact: Breaches of privacy are gaining headline coverage, with reputational damage and significant regulatory penalties being levied on businesses that fail to protect users.



Businesses spend large sums to protect the data they collect

In order to build trust and remain compliant with regulations, businesses that collect and store sensitive user data need significant security budgets and skills to keep it secure.

The impact: The risks and costs associated with data security and privacy can stifle innovation by creating overly-conservative security policies.

Why we need to challenge the status quo?

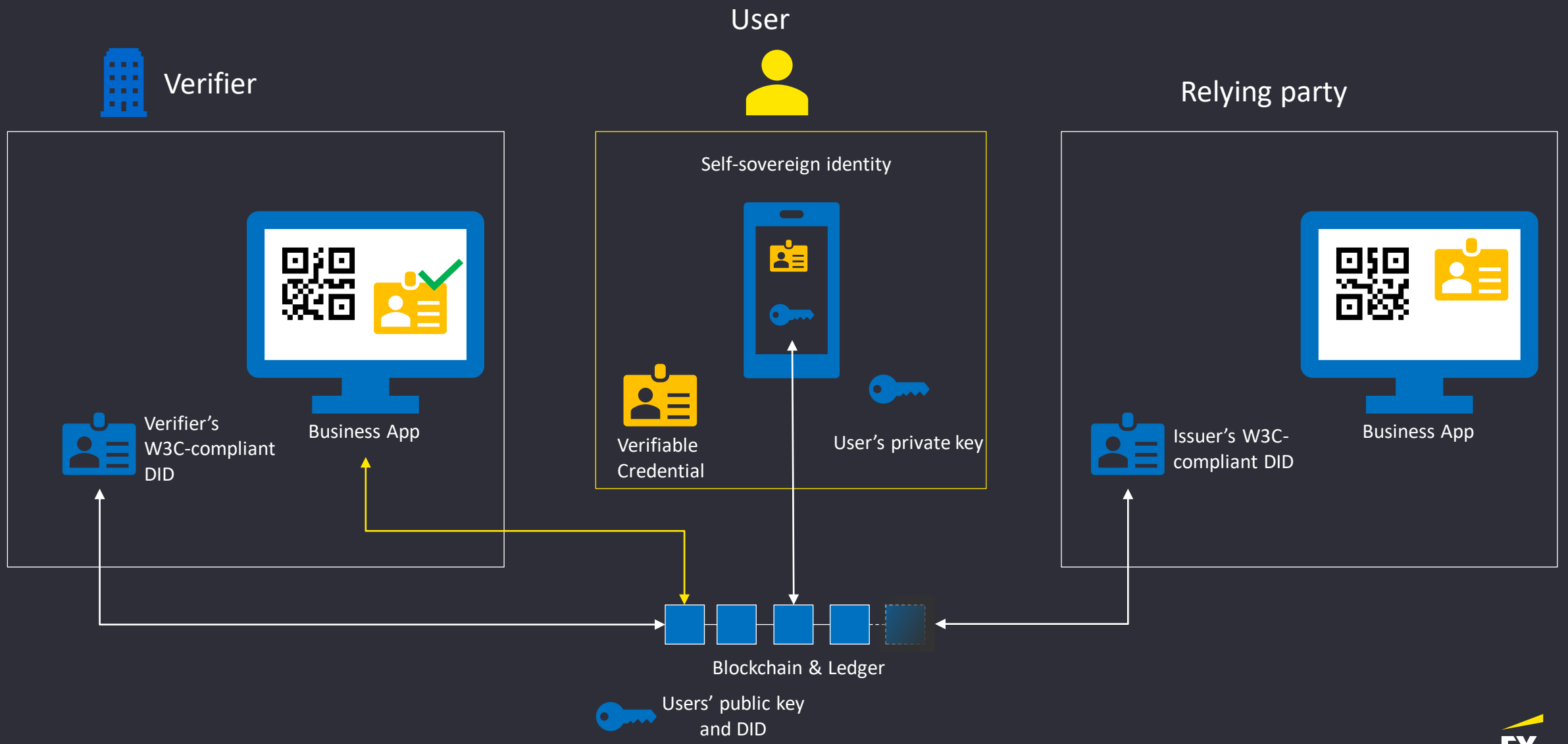
Traditional IAM (Web 2.0)

- Identity and entitlements stored in centralized (e.g., directories, RDBMS)
- Pros:
  - Centralized control over lifecycle and UX
- Cons:
  - Increased liability (in case of a breach)
  - Increased costs (borne by one party)
  - Poor user experience (due to multiple identities)

De-centralized IAM (Web 3.0)

- User owns the identity, and the architecture is distributed on the blockchain
- Pros:
  - Improved cost effectiveness (Distributed across several parties)
  - Diversification of risks (no single point of failure)
  - Improved UX (due to portability)
- Cons
  - User is in control
  - Private keys grant access to everything
  - “Password reset” does not really exist if private keys are lost

The parts of the ecosystem



Example de-centralized identity use cases



Wealth and Asset Management

Leverage a claimant's DID to verify their identity before disbursing payments



Healthcare

Patient can use their DID as a one stop shop to verify identity to book doctor's appointments, check in at the doctor's office and pick up medication



Mortgage Banking

Exchange of DID between the bank and the borrower to verify the integrity of the transaction



Customer Retail IAM

Enable a seamless and private online retail experience, expediting checkout and customer acquisition while retaining privacy



Social Media

Enable users to "sign" a post on an organization's social media account with their portable ID



B2B Transactions

Enable B2B Access for Partners without their own on-premises IDP

See more at: https://www.w3.org/TR/vc-use-cases/

Thank you – Q&A

