The Future of Authentication
April 21, 2017

David Shroyer

Queen CyberSecure

Managing Director

David.Shroyer@queencyber.com

QUEEN ASSOCIATES | QUEEN CYBERSECURE

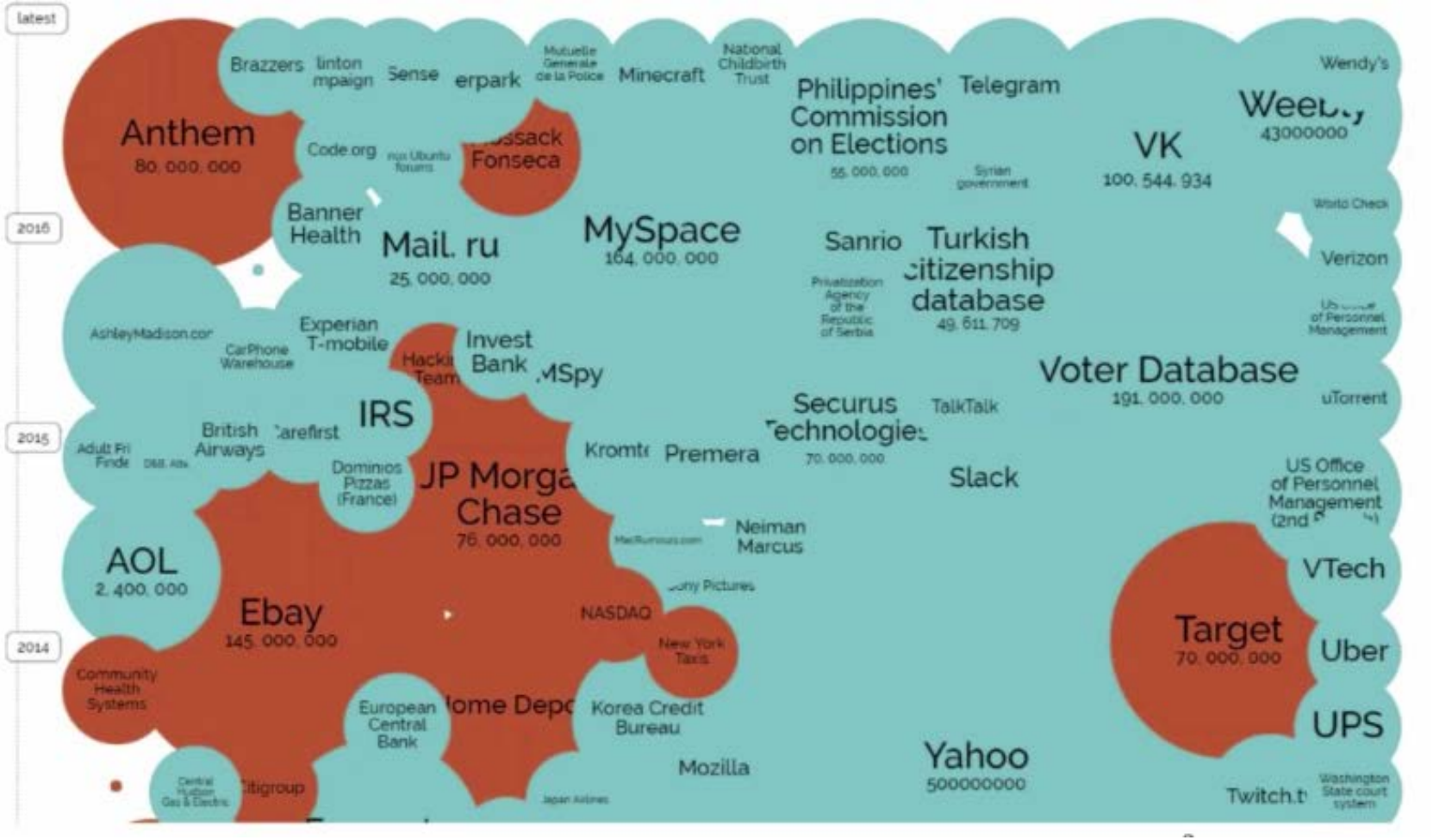
Agenda

Agenda
The Need for Advanced Authentication
How Does it Work?
Benefits
Conclusion

QUEEN CYBERSECURE

The Need for Advanced Authentication

Data Breaches and Magnitude



QUEEN CYBERSECURE

The Need for Advanced Authentication

- Commonly stolen information
  - UID/PW
  - Secret Questions and Answers
  - Credit and Debit Card Numbers
  - CVV Codes
  - Expiration Dates
  - Personal Information (DOB, MMN, DL, Address, SSN)

QUEEN CYBERSECURE

The Need for Advanced Authentication

	Data Element	Standalone Rating
Regulatory Component	Credit / Debit Card Number**	HIGH
	Social Security Number (SSN)	HIGH
	Tax ID	HIGH
	HIPAA HealthCare Data*	MED
	Name (Last and First/First Initial)	MED
	Login ID	MED
Contextually Dependent	Password**	MED
	PIN #	MED
	Security Question Response	MED
	Drivers License/State ID Number	MED
	Home Address	MED
	Date of Birth	MED
	Email Address	MED
	Mother's Maiden Name	MED
	Account Number	MED
	Account balance	MED
	Account transaction history/detail	MED
	CVV/Expiration Date (Credit/Debit Card)	MED
	Credit Score (individual)	LOW
	Phone Number	LOW
	Routing Number/Bank Name	LOW
	Salary	LOW

Transactional Capability
Type and extent of transactions performed (Rank 1 – 12)

1=View single user transactional information only (ex. Canceled checks, activity of charges, etc.)
2=View multi user transactional information only (ex. Canceled checks, activity of charges, etc.)
3=View single user account information (ex. Account #, account balances, etc)
4=View multi user account information (ex. Account #, account balances, etc.)
5=View single user privacy information (ex. SSN, address, beneficiaries, credit report, etc.)
6=View multi user privacy information (ex. SSN, address, beneficiaries, credit report, etc.)
7=Update single user account information (ex. Address, password, dependencies, etc.)
8=Update multi user account information (ex. Address, password, dependencies, etc.)
9=Update single user financial information (ex. Transfer funds between accounts, loan orig, etc.)
10=Update multi user financial information (ex. Transfer funds between accounts, loan orig, etc.)
11=Transfer funds between accounts for single user (ex. ACH & Wire transfers, etc.)
12=Transfer funds between accounts for multi users (ex. ACH & Wire transfers, etc.)

Impact of Risk – *Rank Each Category*
(Rank: 1=Low, 2=Medium, 3=High, 4=Critical)

- Legal/Regulatory: Direct legal or regulatory violations
- Financial: Direct financial losses or associated costs
- Reputation: Loss of customer confidence
- Harm: Physical harm to the operations of the business
- Personnel: Direct impact on personnel, work environment, hiring/retention or safety
- Unauthorized Exposure: Release of sensitive, proprietary, or regulated information

Sensitivity of Information Accessed:
(Rank: 1-3)

Data Sensitivity is determined using the matrix that has been developed for other BANK risk assessments like; Data Classification, Operational Risk Reviews, and Third Party Assessment Program. The model is outlined in Appendix B.
1 = Low – Information has a low data sensitivity score
2 = Medium – Information has a moderately high data sensitivity score
3 = High – Information has a high data sensitivity score

Data Risk increases with more data breaches

Transaction Risk Increases with more functionality

QUEEN CYBERSECURE

How is Advanced Authentication Being Used?

IDT

- Mule Accounts
- New Credit
- Social Engineering

ATO

- Account Access
- Money Movement
- Credential Change

IT'S TAX SEASON!

- IRS and Tax Services

QUEEN CYBERSECURE

The Need for Advanced Authentication

ATO IS ON THE RISE IN MANY MARKETS

Chip Cards Introduced

QUEEN CYBERSECURE

Understanding Authentication

- Advanced authentication requires two-factors

QUEEN CYBERSECURE

Understanding Advanced Authentication

- Advanced Authentication Attributes

FRICTIONLESS

CONTEXTUAL

ADAPTIVE

Consumers will adopt solutions that ease the burden of remembering passwords or carrying tokens

QUEEN CYBERSECURE

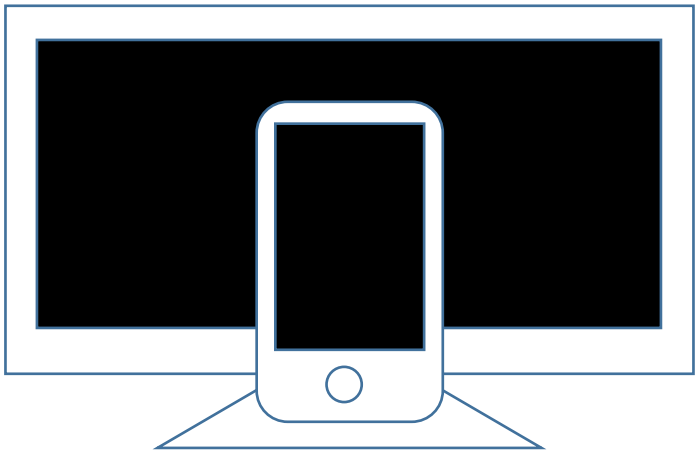
Understanding Advanced Authentication

FRICTIONLESS
INVISIBLE TO THE USER

Is device authorized for this account?

Where is device located?

How many accounts has device accessed?



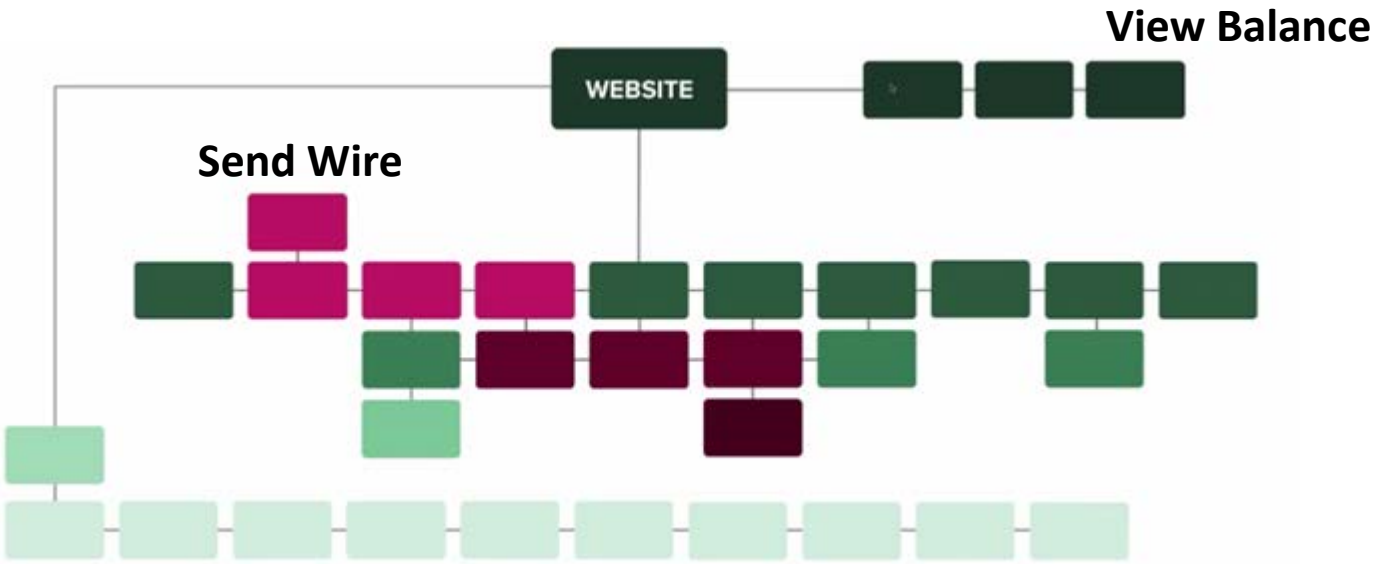
Is this a person or a bot?

Does device have history of fraud?

Is device hiding from detection?

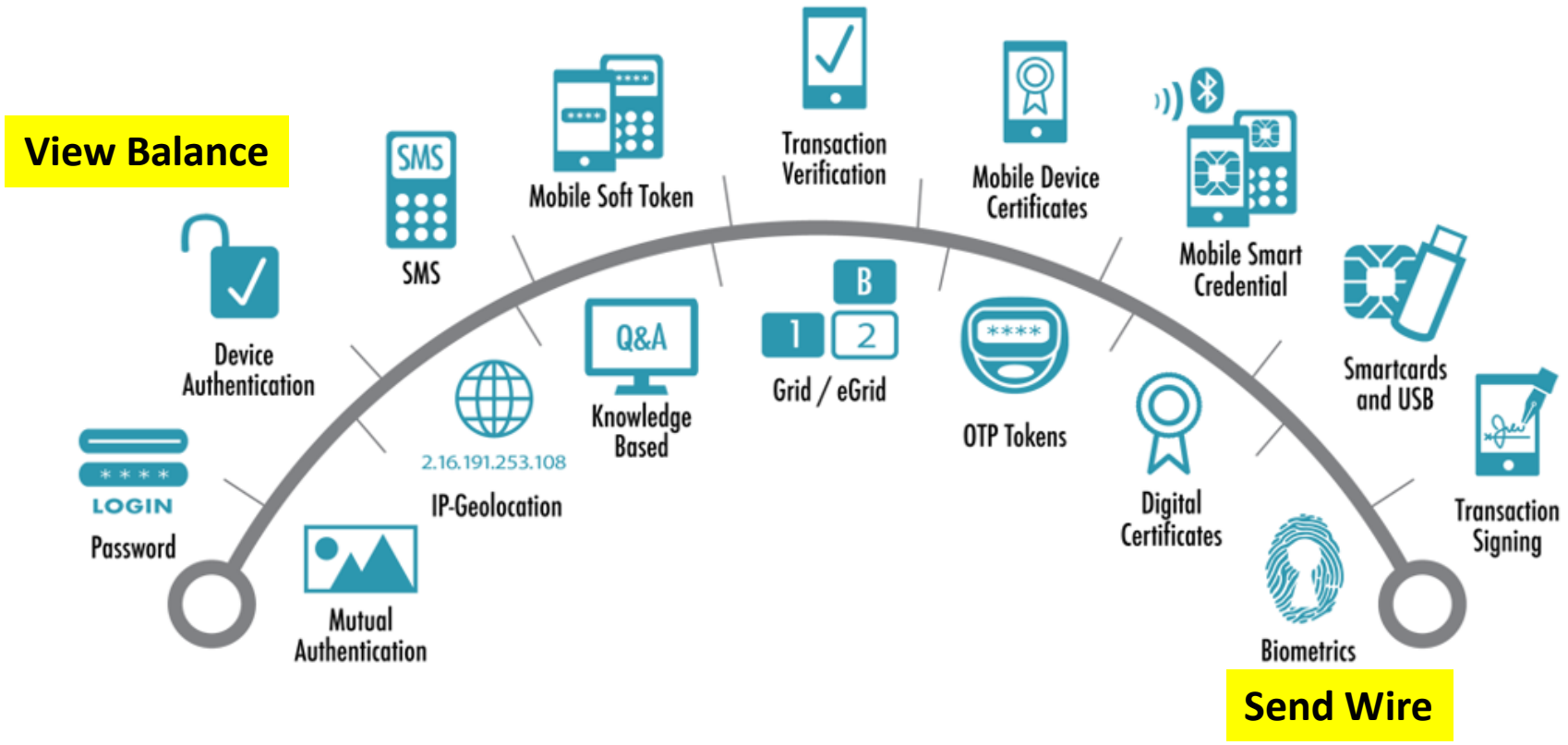
QUEEN CYBERSECURE

CONTEXTUAL
WHERE IS THE GREATEST RISK?



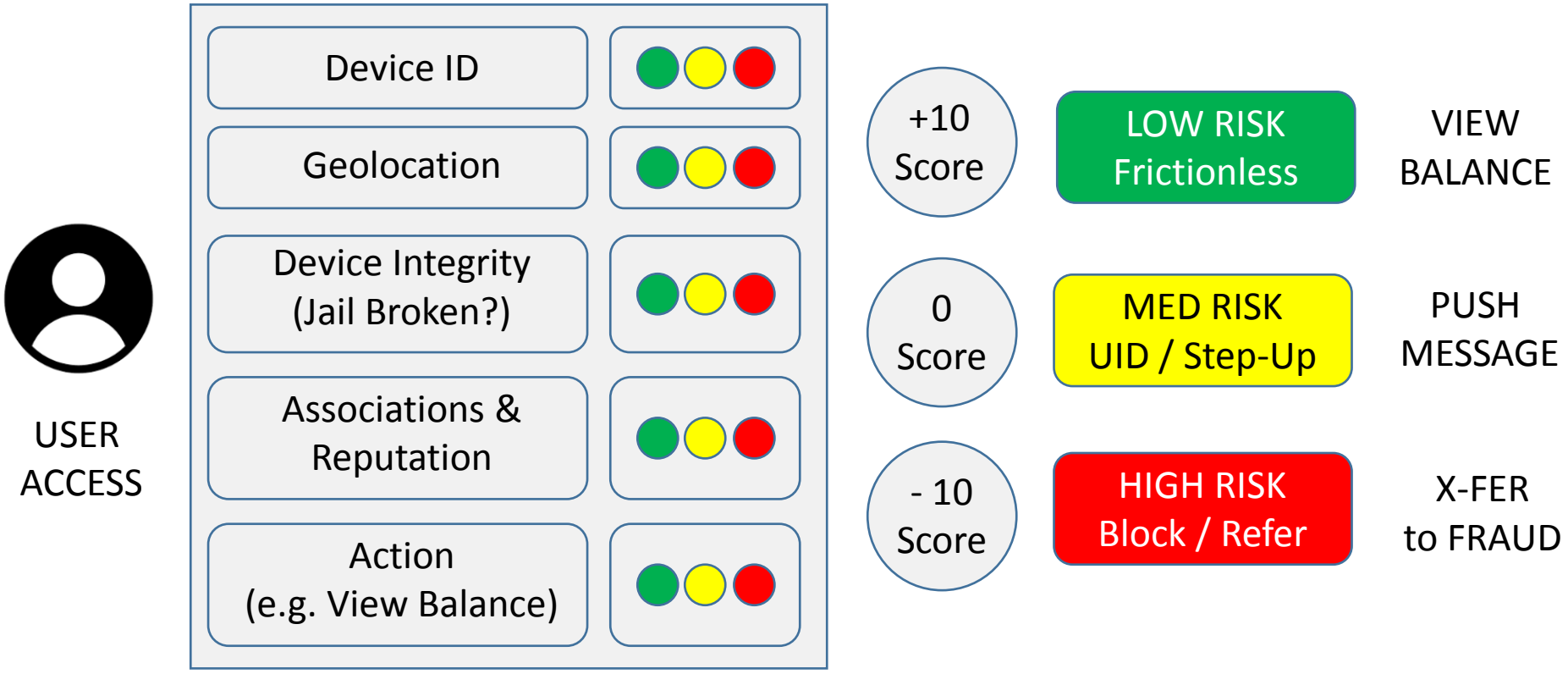
Understanding Advanced Authentication

ADAPTIVE
WHAT YOU DO, DICTATES THE AUTH YOU NEED



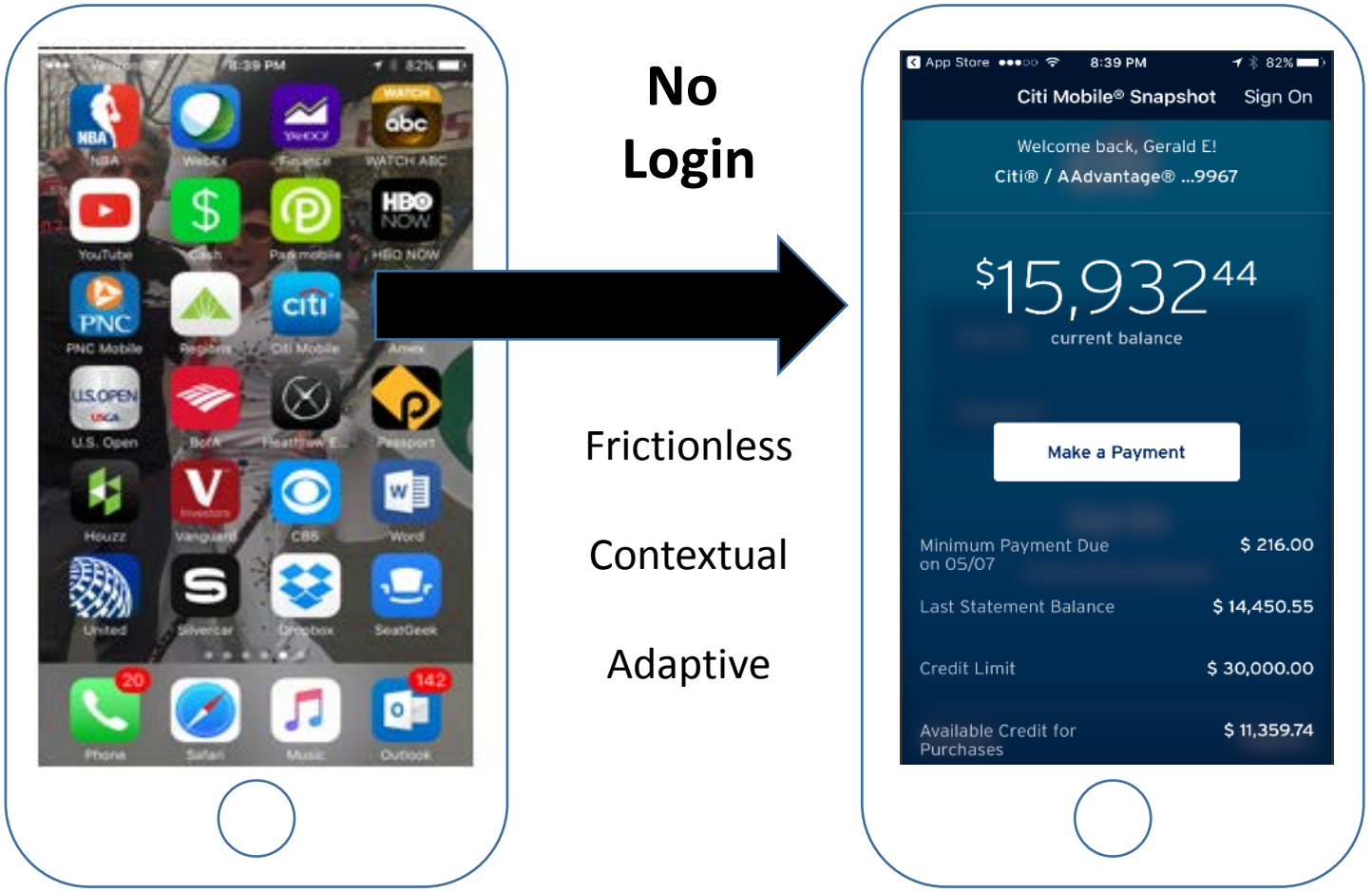
QUEEN CYBERSECURE

How Advanced Authentication Works



QUEEN CYBERSECURE

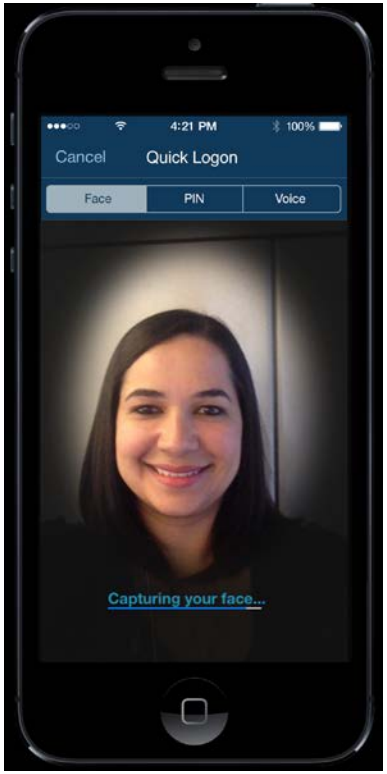
How Advanced Authentication Works

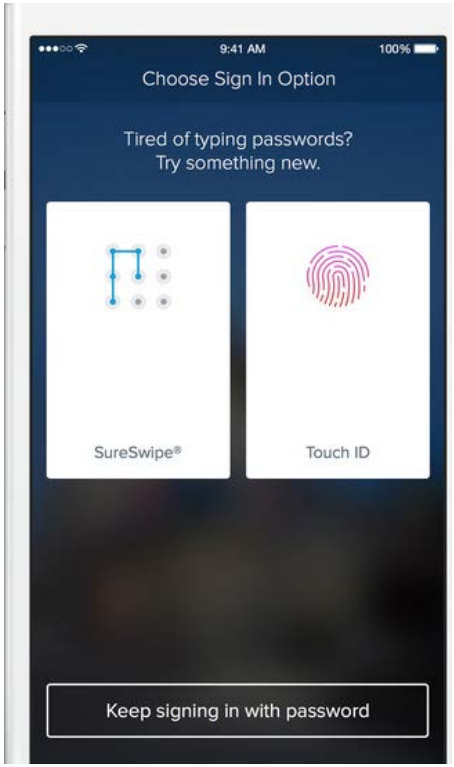


QUEEN CYBERSECURE

How Advanced Authentication Works

- A Mobile Example





QUEEN CYBERSECURE

How Advanced Authentication Works

- Next Gen concept announced yesterday by MasterCard

MasterCard debuts a credit card with a fingerprint sensor to fight fraud

April 20, 2017

http://www.zdnet.com/article/mastercard-debuts-credit-card-with-a-fingerprint-sensor/

QUEEN CYBERSECURE

How Advanced Authentication Works

Cross Channel Awareness

	IVR	CALL CENTER	WEB	APP
Low Risk	ANI + Anti Spoofing	ANI + Anti-Spoofing	UID + Device ID + Context	Device ID + Context
Action	Hear Balance	Hear Balance	View Balance	View Balance
Med Risk	+ Debit PIN	+ Push OTP to App	+ Push OTP to App	+ Touch ID
Action	Bill Pay	Bill Pay	Bill Pay	Bill Pay
High Risk	+ Voice Print	+ Push OTP to App	+ Push OPT to App	+ Touch ID
Action	Change PII	Change PII	Change PII	Change PII

QUEEN CYBERSECURE

Benefits of Advanced Authentication

QUEEN CYBERSECURE

Conclusion

- A Four-Step Plan to Evaluate Customer Authentication for your Sites:

1. For brand managers, product owners, or web experience managers, understand where the greatest risk is on your site;

2. Understand what benefits would be realized if your customers experience less friction;

3. Assess the impact of a frictionless, contextual and adaptive approach to your current authentication methods; and

4. Create your plan to retire passwords and secret questions.

QUEEN CYBERSECURE

Questions?

David Shroyer

Queen CyberSecure

Managing Director

David.Shroyer@queencyber.com

(980) 253-3525

QUEEN CYBERSECURE