Fraud & Identity
Trends and Best Practices

Stacey Wishowsky– Sr. Business Consultant
Fraud and Identity Advisory Services
October 2019

Market Trends

Experian Insights & Credit Union Feedback

Drive Growth:

- Increase deposits, members
- **Safely lend beyond prime**
- Expand loan mix (card, personal)
- Increase # of direct loans
- Grow small business lending
- Improve loan yields
- **Reduce costs/efficiency ratio**

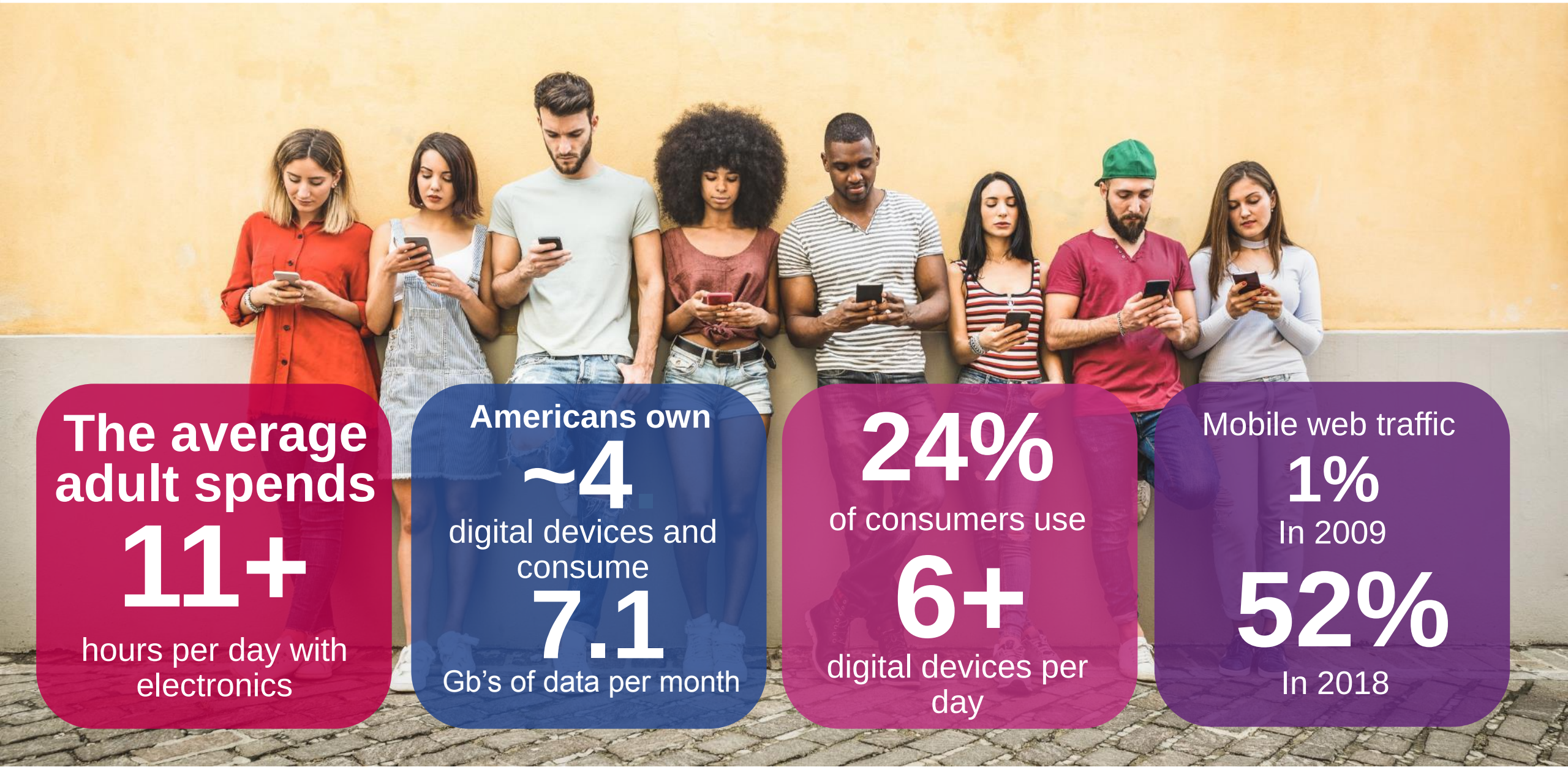
Minimize Risk:

- **Prevent fraud across channels**
- Protect member identities
- **Safeguard Brand and loss lines**
- Prepare for economic downturn
- CECL preparedness

Improve Member Experience:

- **Leverage automation**
- Serve more members
- Enhance experience via digital
- **Decision faster; reduce friction**

Today’s interactions with consumers occur on a screen



The average adult spends

11+

hours per day with electronics

Americans own

~4

digital devices and consume

7.1

Gb’s of data per month

24%

of consumers use

6+

digital devices per day

Mobile web traffic

1%

In 2009

52%

In 2018

Research, Impact, and Considerations

80%

US businesses with more online fraud in the past year

2 in 5

Consumers worldwide that have already experienced a fraudulent online event (highest incidence is in the US)

Data breach notifications in 2017

61.1 M

People that use the same password across multiple online accounts

81%

87%

Customers think brands should put more effort into providing a seamless experience

65%

US consumers that believe obvious security measures are extremely or very important

Research, Impact, and Considerations

14.4 million

identity fraud victims in 2018 - Javelin

Account takeover totaled

$4.0 billion

in 2018 – Javelin

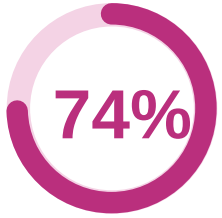
60% of financial institutions report first party fraud as the prominent source of fraud loss – Payment Journal March 2018

New account fraud losses rose to

$3.4 billion

in 2018 – Javelin

of consumers would provide even more information to businesses if there was a perceived benefit to them – for security or for convenience



of consumers are more confident that physical biometrics will protect their information over passwords

Regulatory Landscape

Objectives

- Positive customer identity validation
- Understand the business portfolio profiles and risk
- Validation/authentication of high risk customers
- Avoid enforcement actions and risks
  - Fines, sanctions, civil penalties, brand reputation

Requirements and trends

- Streamlined: enterprise strategies, vendor sources
- KYC/CIP Acquisition and account management
- Reduced subjectivity
- Synthetic Identities
- Data integrity/accuracy
- Economic Growth, Regulatory Relief and Consumer Protection Act (S. 2155)
  - Consent Based Social Security Verification (CBSV)
- Customer Education

Strategic and operational aspirations

- Consistent, repeatable processes
- Standardize oversight capabilities
- Granular ID result matching, defensible results
- Leverage at an enterprise level
- Detailed reporting, demonstrable results

Regulatory body priorities

Fraud Landscape

Overview

- Increased 1st Party fraud and ATO fraud
- Synthetic Identity; lifecycle impact
- Identity Fraud: a crime of complete impersonation(1)
- Inquiry manipulation: Exposure to Stacking
- Authorized User – 'piggybacking'
- Call center vulnerabilities: top 4 fraud concern(2)
- Contextual assessments and authentication
    - Passive and active observations and inputs combined with external validation
- Leveraged investments
    - Infrastructure for rapid deployment, strategy maintenance
    - Reduced vendor and process complexity
- EGRRCP (S. 2155)
- Increased consumer education

Strategic Focus

Expansion

Synthetic and First Party

Customer Journey

By the Numbers

- 55% risk managers list Identity fraud as area of greatest concern in 2018(2)
- Call Center fraud increased 113%(3)
    - Over 60% of ATO losses involve the call center
- The cost for each dollar of fraud losses increased 15% from 2016(4)
    - $2.67: Finance Services, $2.78: Credit Lending

Sources: (1) Javelin, Feb 2018
(2) Gartner, Apr 2018
(3) Pindrop 2017 Call Center Fraud Report
(4) LexisNexis® Risk Solutions 2017 True Cost of Fraud℠

Key Fraud Types

- First-Party Fraud
- Synthetic Identity (SID)
- Third-Party Fraud (ID Theft)

First Party Fraud

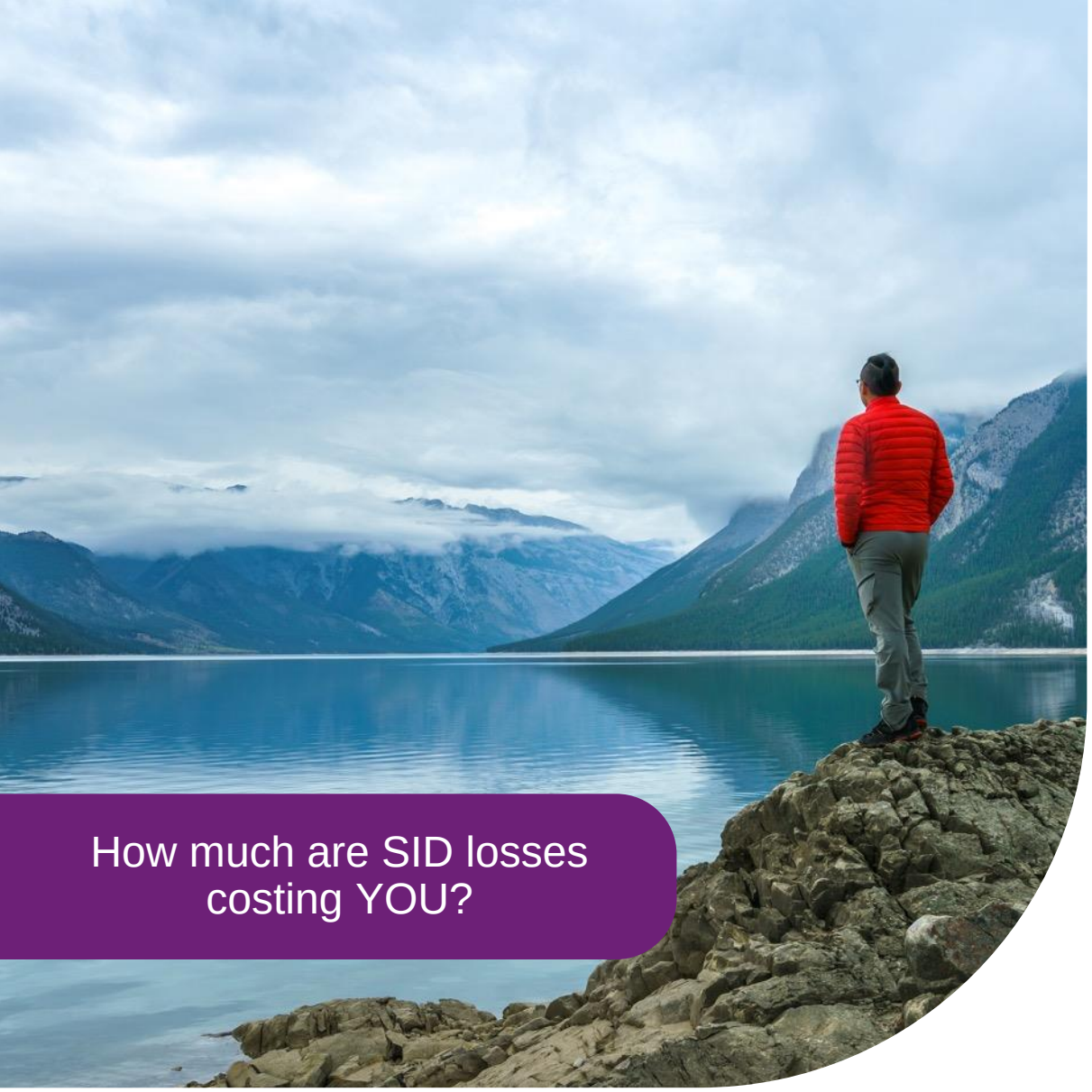
- Losses align to Credit P&L
  - Impact throughout lifecycle
- Non-malicious intent adds complexity
- Protection of Brand, growth and consumers
- Processes must not raise UDAAP concerns

First Payment Default
Loan Stacking
BustOut
Synthetic Identity

60%
of financial institutions report first-party fraud as the biggest source of fraud losses[1]

10% to 35%
of bad debt is a result of first-party fraud[2]

[1]Payments Journal, March 2018
[2]FICO, March 2017



Synthetic Identity
Impact and opportunity

- **20% of credit losses***
- Average > $10k loss per account**
- ~ $800 million in U.S. credit card losses in 2017**
  - Estimated $1.2 billion by 2020
- $300 million + attributed to authorized users***
- Government Accountability Office (GAO) industry forum
  - Estimated losses to individual institutions of $50-250MM annually

*Auriemma 2017 ** Aite 2017/2018 ***Experian 2017

Synthetic ID

- Differing methods of how to detect / measure impact
- Inconsistent identity verification
- No agreed upon definition across institutions or regulators
- Straight roller, nurturer, bust out
- Authorized users, data furnisher schemes, credit repair

Creation
Authorized user
Retail card
Small credit line

Incubation
3-24 months
Act normal
Lay low

Credit/loan stacking
High velocity inquiries
Sudden activity change
Credit concentration

Bust out
High utilization
Recent delinquency

Authorized user farming studies

Summary findings

Increasing SID yield – AU user rotation

Charge off rate on subsequent accounts increases > AUs; 48.3%

Loss correlation

One known consumer:

- 18 AUs added over three-year study
- $125K in losses, to date, on 13 of the accounts opened by authorized user

Stolen Identities are more accessible than ever

Cost of Stolen Identities is minimal

- Globally, PII (personally identifiable information) is increasingly at risk and being monetized by bad actors
- Bad actors are more efficient at:
  - Phishing schemes
  - Data Breaches
- Early 2019 estimated “fullz” cost*:
  - $1-3 for a fullz without bank info
  - $50-$70 for “fullz” plus bank account information
- PII should not be solely relied upon for ID verification
  - Alternative data and behavior incorporated

Identities, Passports, Social Security Cards and Other Documents

	Price in 2013	Price in 2014	Recent Prices
US Fullz	$25	$30	$15 – $65
Fullz (Canada, U.K.)	$30 – $40	$35 – $45	$20 (Canada) $25 (U.K.)
U.K. Passport Scan			$25
Physical Counterfeit Passports (non-U.S.)	N/A	$200 – $500	$1,200 to $3,000 (European)
Physical Counterfeit Passports (U.S.)			$3,000 to $10,000
Templates for U.S. Passports			$100 – $300
New Identity Package, including scans of Social Security Card, Driver’s License and, matching utility bill		$250; matching utility bill an additional $100	$90
Physical Counterfeit Social Security Cards		$250 – $400	$140 – $250
Scans of Counterfeit Driver’s License			DL Scans $14 – $20 (U.S.) $14 (U.K., CANADA)
Physical Counterfeit Driver’s License (France)			$238
Physical Counterfeit Driver’s License (U.S., U.K., Germany, Israel, International Driver’s Permit)		$100 – $150	$173

Chart: Dell Securesystems, 2014

Note: A “fullz” is a combination of: Individual’s name, Date of birth, Social Security number, Phone number, and often includes banking information

* Source: Aite Group Sr. Cybersecurity Analyst, Alissa Knight)

Best Practices - Contextual Risk Assessment

Right-time solutions, authentication options, a secure customer journey

Comprehensive, omni-channel view of the consumer with contextual risk assessments

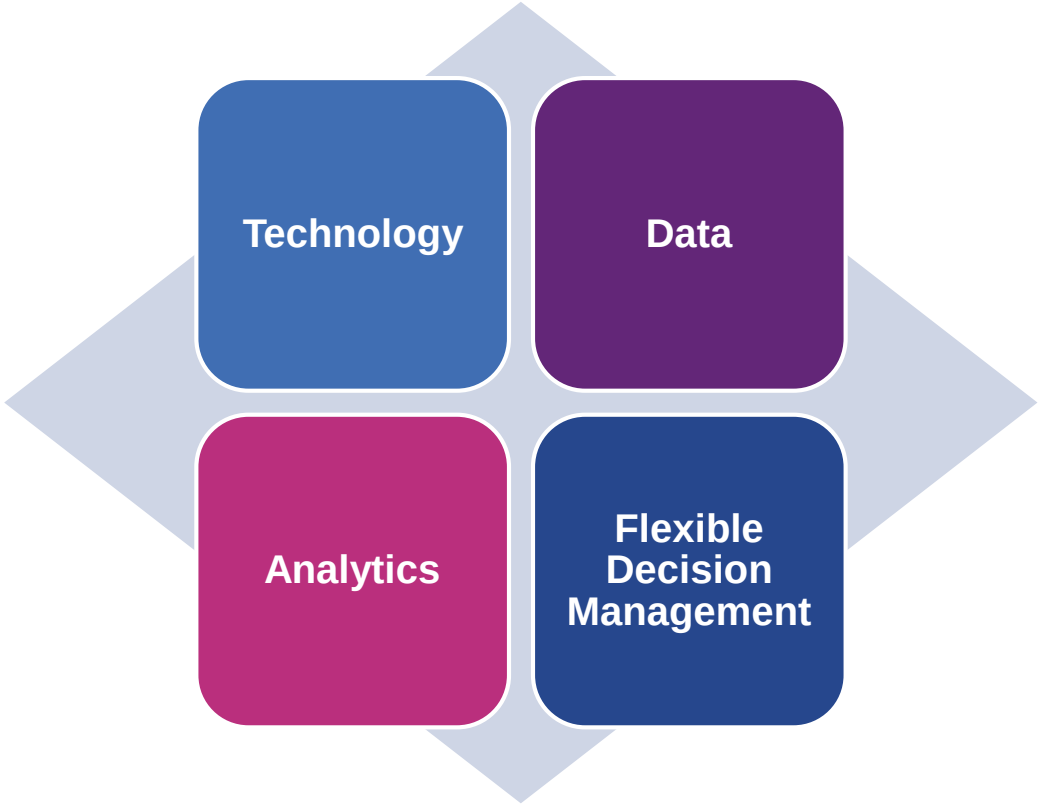
Consistent, enterprise strategies, policies and procedures

Authentication incorporates active and passive inputs that are flexible to reduce fraud and customer disruption

Analytics and data throughout processes

Revolutionized technology stack: speed to market, automation, and future-proofed

Trusted partnerships that provide industry insights and best-in-class capabilities



Current Best Practice tools and Controls

APPLICATION REVIEW

- Credit and BustOut models
- Fraud models
- Thin file scrutiny
- ID Interrogation
- Digital intelligence
- Negative files
- Documentation

PAYMENT MONITORING

- $ threshold
- Max pay permissions
- OTB holds
- NSF policy
- *Deposits
- *ATM

TRANSACTION MONITORING

- Fraud models/strategies
- Utilization
- CLI constraints
- Digital intelligence
- High risk event review
- Multi-layer authentication
- Authorized user policy
- Collection campaigns

AUTHENTICATION

- Passive
  - PII
  - Device
  - Email
  - Biometric
- Active
  - Password/PIN
  - KBA
  - OTP
  - Document
  - Biometric

Digital identity validation and customer experience

Balance required

66% of consumers said, "I like all the security protocols when I interact online because it makes me feel protected."

India	S. Africa	Australia	U.S	France	U.K
76%	74%	70%	69%	67%	66%
Spain	**Singapore**	**Brazil**	**China**	**Turkey**	**Overall**
64%	63%	63%	62%	56%	**66%**

Q: Please indicate how strongly you either agree or disagree [with each of the following statements] on the scale provided - disagree strongly, disagree, neither agree nor disagree, agree, strongly agree.

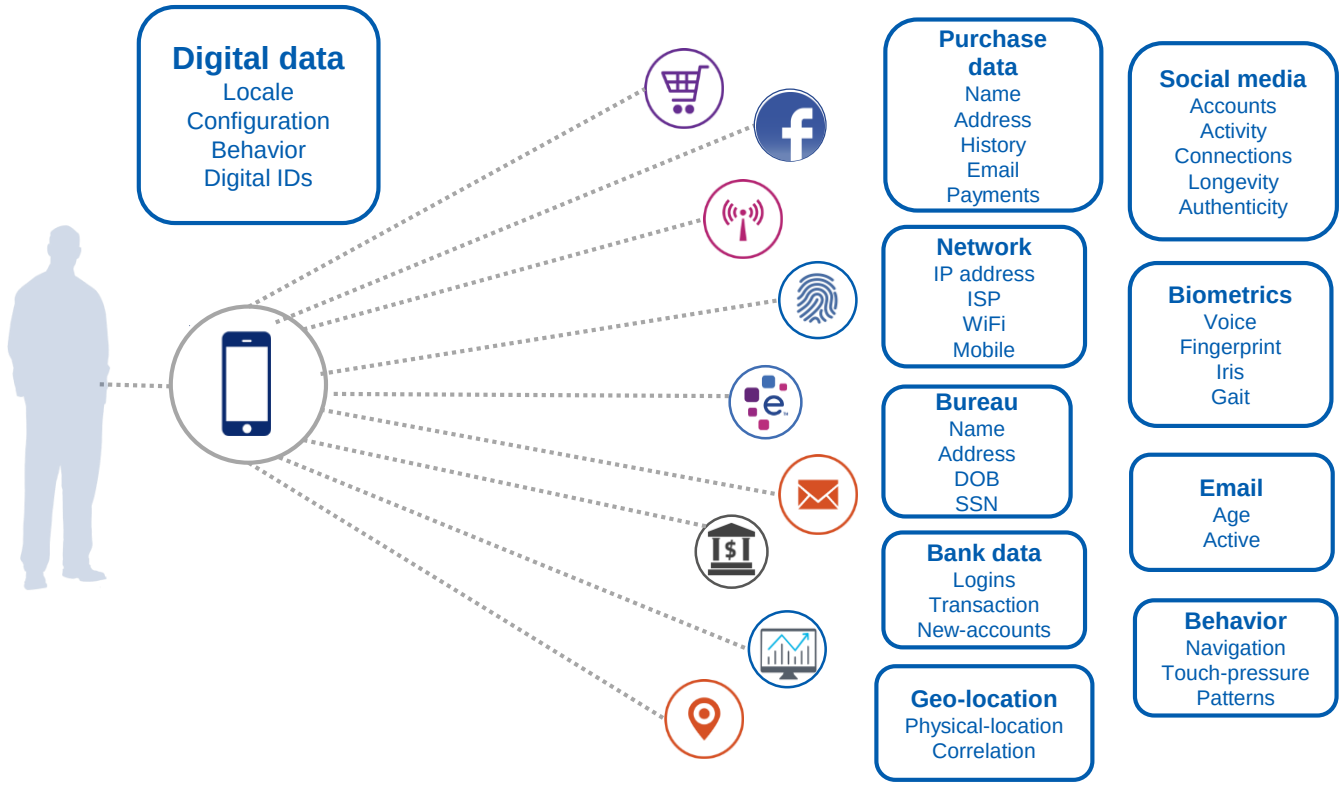
***Experian 2018 Global Fraud and Identity Report, 66% of consumers surveyed said they like security protocols when online because they feel protected…**

42% of millennials said they would conduct more online transactions if there weren't so many security hurdles to overcome...

...versus **30%** among those 35 and older

The Ultimate Consumer ID Profile…
…To Recognize Your Customer

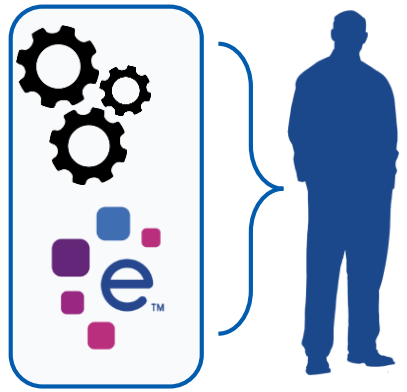
…Aggregate data via Experian Global ID Hub… CrossCore



Traditional ID solutions use basic Bureau-based personal identification information – ***"Essential, but not sufficient"***

The market requires richer, ***context-based data assets***

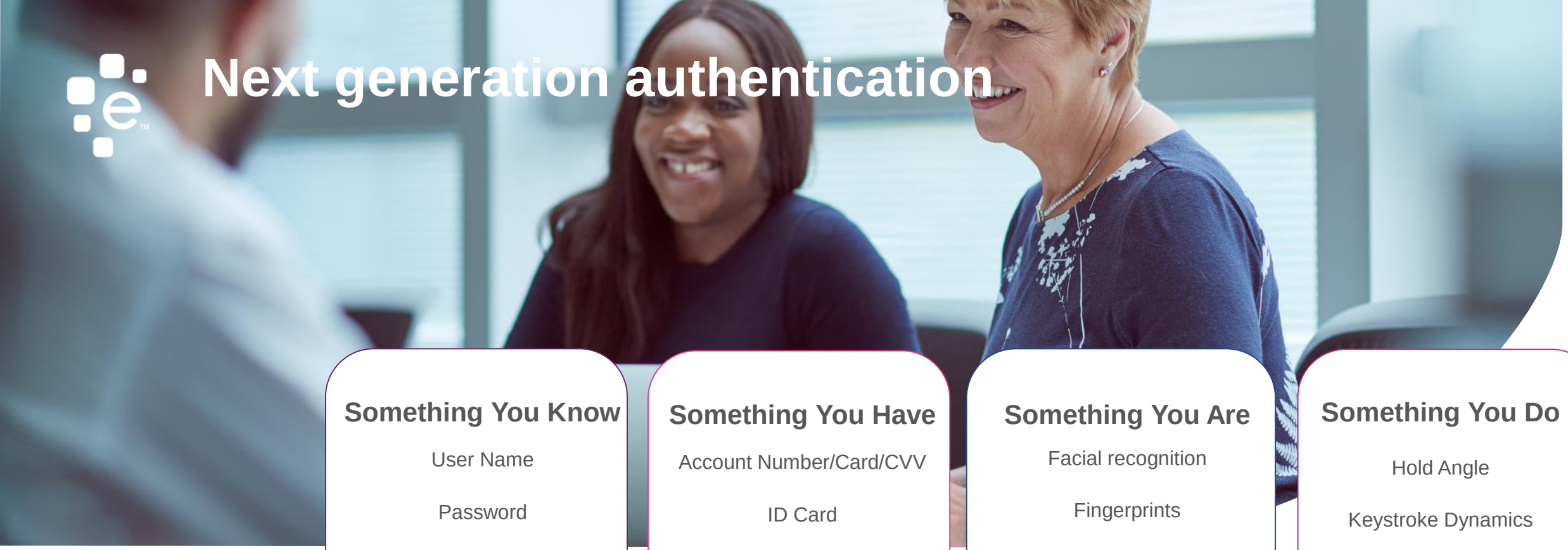
Leverage new ***emerging alternative data sources***



…Create the ultimate ***consumer identity profile***

"I can tell you with 100% conviction that identity proofing is the biggest fraud problem out there"
– Avivah Litan, Gartner

Next generation authentication



Something You Know

User Name

Password

PINs

One Time Passcode

Out of Wallet Questions

Captcha

Something You Have

Account Number/Card/CVV

ID Card

Tokens

Badges

USB Keys

Smart Cards

Device

Something You Are

Facial recognition

Fingerprints

Iris/retina scans

Voice prints

Heart Rate

Vein print

Something You Do

Hold Angle

Keystroke Dynamics

Mouse Movement

Screen Navigation

Touch Pressure

Authentication

Typical authentication “feels” heavy-handed:

- Managing passwords - by 2020, consumers estimated to have 207 passwords
- Cookies used to recognize devices – when cleared, device becomes “unrecognized”
- KBA questions are often forgotten/inaccurate – OR – Fraudsters know the answers
- Being pushed from one channel to another to resolve issues (online to call center, to branch)
- Repeat visits to the same business site require the same repeated processes every time

Ideal experience:

- My device has been seen before – “Auto-login”
- Even if cookies are deleted, the consumer or their device proxy is still recognized
- Click to enter: “Welcome Back!”
- Additional requests and actions are risk assessed appropriately to introduce additional authentication that “makes sense” to the member

Passive Authentication! Contextual Risk Assessment! Less Friction!

The future customer experience

A contextual assessment that with the right technology will **support growth, drive down risk** and **decrease customer friction**

Grow your credit union

Drive down risk

Decrease customer friction

"By 2022, Digital Businesses with **GREAT CUSTOMER EXPERIENCE** during identity corroboration **WILL EARN 20% MORE REVENUE** than comparable businesses with poor customer experience" - Gartner Future of Identity Dec 2018**

Experian Advisory Services can help with fraud consulting options that meets your budget

Standard engagement topics:

Onboarding and acquisition

- Synthetic ID
- First Party Fraud (FPD/Bust Out)
- Fraud Application (3rd Party Risk)

Account management

- Account Take Over
- Credential Stuffing
- Payment Fraud/Bust Out
- Synthetic ID

Regulatory

- Customer Identification Program (CIP)
- Red Flag Rules program

Authentication

- Acquisition
- Account management
- Call Center Account Takeover and Social Engineering

Virtual fraud education

- Virtual fraud training webinars that provide insight into industry trends and best practices

*** Custom engagements can be aligned to your needs and goals with topics specific to your organization**

Key Benefits

- Expand your team's skillset and knowledge with minimal investment
- Address immediate gaps or opportunities with quick hit recommendations
- Stay up to date on the latest and greatest tools and solutions, fraud trends, and regulatory guidelines
- Receive thought leadership insight into industry best practices

Expand Potential

"To get Game-Changing results, start focusing on Game-Changing thoughts."

– Robin Sharma