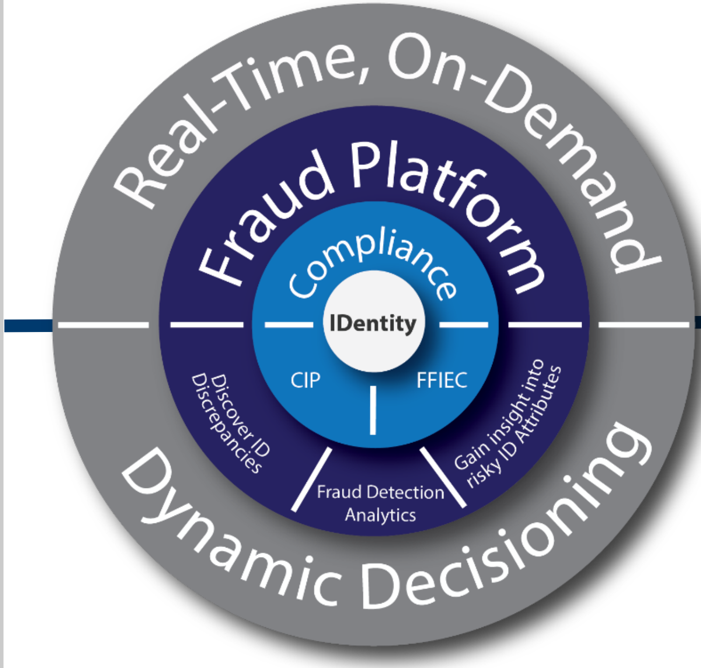

Real-Time, On-Demand
Fraud Platform
Compliance
IDentity
CIP
FFIEC
Discover ID Discrepancies
Fraud Detection Analytics
Gain insight into risky ID Attributes
Dynamic Decisioning

Mobile Identity and Driver's License Scanning Technologies

Federation of Tax Administrators 32nd Annual Technology Conference

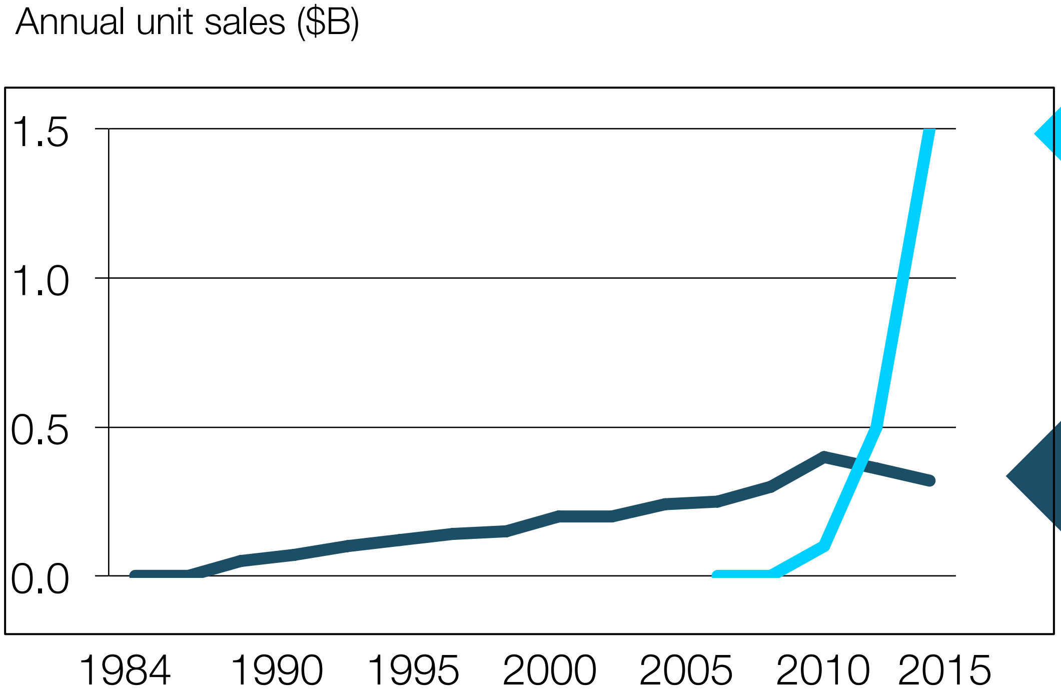
John Dancu

CEO

jdancu@idology.com

IDOLOGY

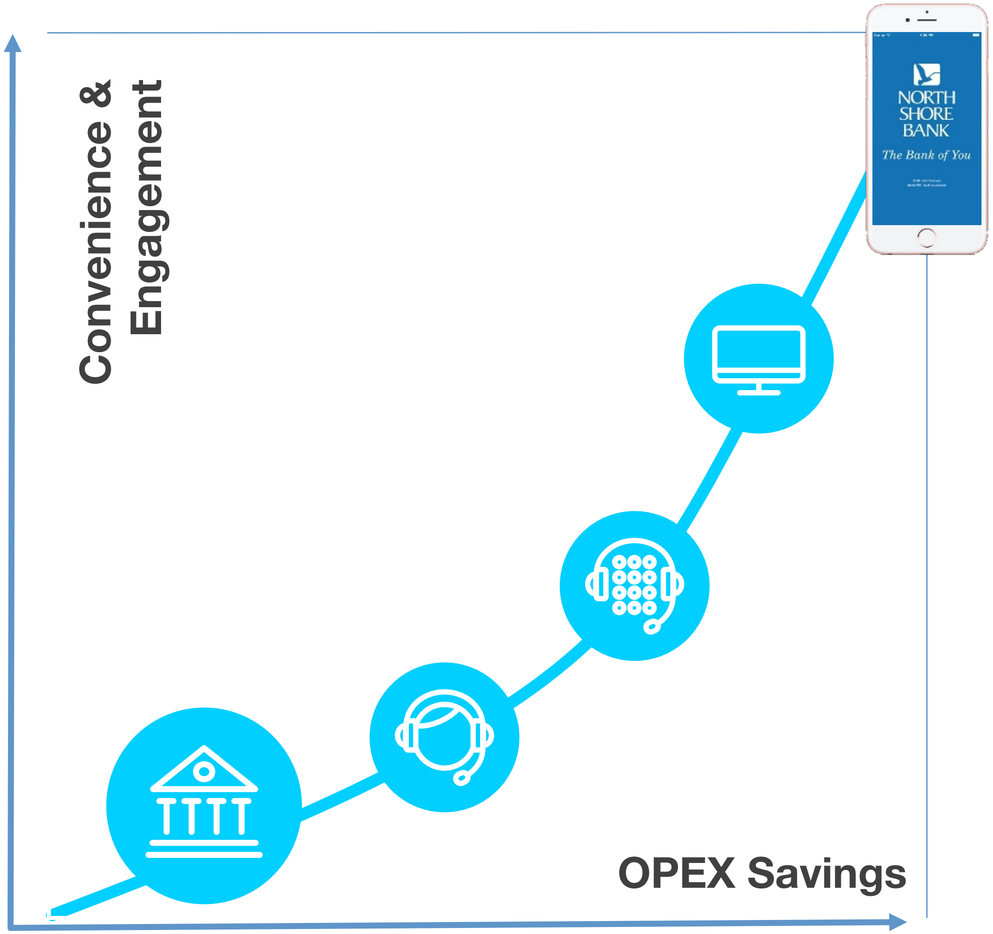
Mobile is now the *preferred* platform



Smartphones
(1.5B shipped)

PCs
(300M shipped)

The dream of “self-service”



$3 to process a check in a branch.
3 cents on the phone.

WELLS FARGO

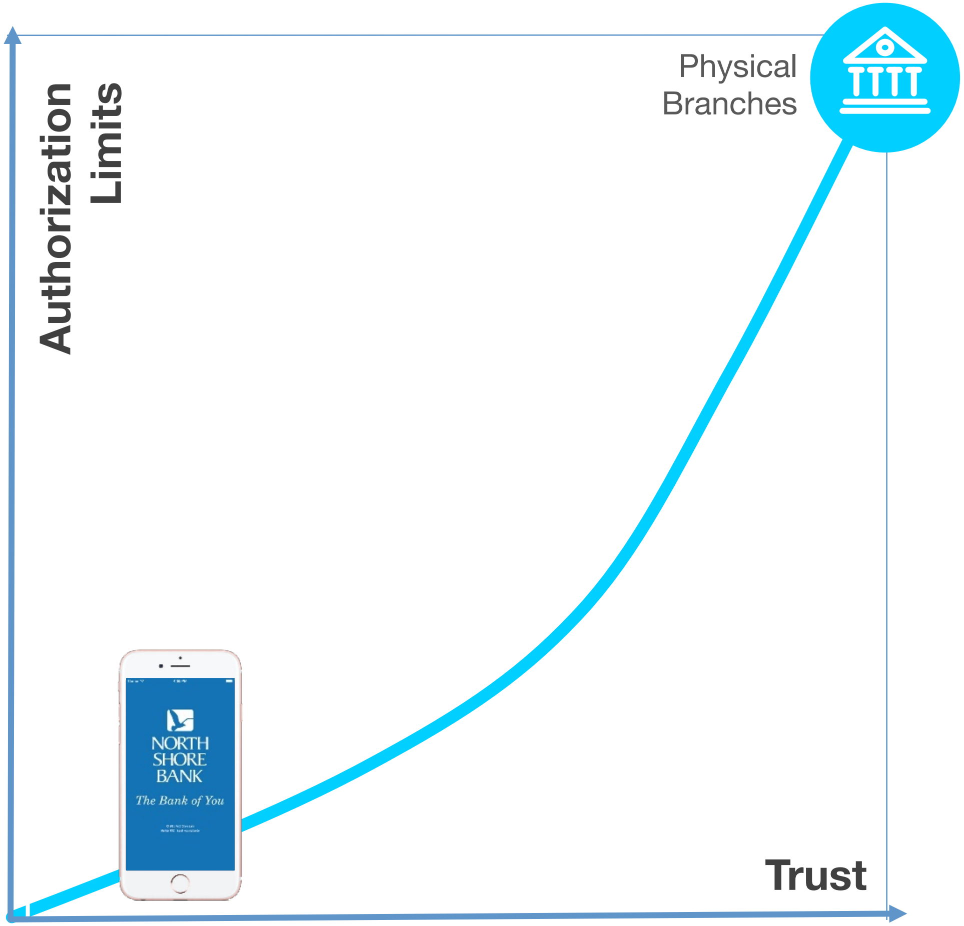
THE WALL STREET JOURNAL.

Bank Branches in U.S. Decline to Lowest Level Since 2005

Banks Cutting Branches as They Trim Costs, Boost Mobile Services

http://www.wsj.com/articles/bank-branches-in-u-s-decline-to-lowest-level-since-2005-1412026235

Yet, mobile is still the *least trusted*



Tellers and agents have $100K+ authority. Mobile is limited to $5K

citi

The friction that is added to tenure accounts and transactions leaves $300B in revenue on the table each year

Aite

“Trust” in mobile starts with understanding how mobile is substantially different than PCs

In 2015

30 Million

Phone numbers were “recycled” … 10M changed their phone #s

80 Million

Consumers switched phone companies

130 Million

Activated new smartphones

THE WALL STREET JOURNAL.

Wrong Number? Blame Companies' Recycling

By Alyssa Abkowitz | Posted 2011-12-01

Some advice for aspiring Hollywood movie moguls: When seeking a big distribution deal, make sure you dial the right phone number.

Cara Bohon, a clinical psychologist who lives in West Hollywood, Calif., was fielding several calls a month intended for an independent film distributor—one known for kung fu movies and "action sports entertainment."

It wasn't long before Ms. Bohon figured out she was the owner of a "recycled" phone number. She says she's more amused than annoyed, so she hasn't changed her number. Still, she adds, "I almost want to tell [callers] they won't watch your film anyway."

http://www.wsj.com/articles/SB10001424052970204012004577070122687462582

eWEEK

NIST Says SMS-Based Two-Factor Authentication Isn't Secure

By Michelle Maisto | Posted 2016-07-27

Updated guidelines from the National Institute of Standards and Technology say SMS-based two-factor authentication should be banned.

While Google has encouraged users to enable two-step authentication within Google Apps, to add "an extra layer of security," the U.S. National Institute of Standards and Technology updated it Digital Authentication Guidelines (DAG) July 27 and now reports that two-factor verification over SMS isn't secure and should be banned.

http://www.eweek.com/security/nist-says-sms-based-two-factor-authentication-isnt-secure.html

9 MOBILE IDENTITY THEFT VECTORS

1. PORT

Fraudster social engineers the mobile network operator call center to port ownership of phone number from victim to himself. When one time passcode is sent, it is sent to fraudster controlled phone number.

2. ANI SPOOFING

Fraudster calls into bank call center pretending to be calling from victim's phone number.

3. RECYCLING PHONE NUMBERS

Fraudster sets up new phone numbers in attempt to receive one which is recycled and is currently attached to a victim's tenured account at a bank.

IS YOUR PHONE IDENTITY SAFE?
1 PORTS
2 ANI SPOOFING
3 RECYCLING PHONE NUMBERS
4 DEVICE CLONING
5 CALL FOR-WARDING
6 SMS INTER-CEPT
7 SIM CLONING
8 SIM SWAPS
9 VOICEMAIL HACK
0

4. DEVICE CLONING

Fraudster makes a software image of the device in order to impersonate the device from a software perspective and fool device fingerprinting solutions. Rooted/jailbroken devices running Android most susceptible to this.

5. CALL FORWARDING

Fraudster enables call forwarding on the victim's phone so that voice calls from the bank terminate at a phone number controlled by them, allowing them to receive verification calls.

6. SMS INTERCEPT

Fraudster intercepts inbound (or mobile terminating) SMS communication from bank to victim.

7. SIM CLONING

Extremely difficult to do and requires knowledge of secret Ki values. SIM values from victim are copied to fraudster SIM so fraudster can impersonate subscriber on the network and obtain all incoming communication.

8. SIM SWAPS (WITHIN SAME MNO)

Similar to device cloning but the 'legal' hardware version of it. Fraudster social engineers the mobile network operator call center with stolen PII/KBA to deactivate existing users SIM and activates a device in their possession in order to hijack all mobile communication.

9. VOICEMAIL HACK

Fraudster breaks into victim's voicemail (obtains victim's voicemail pin, if even set at all etc...). Fraudster causes mobile voice one time passwords sent to phone to go to voicemail (either through DDOS of mobile calls or time of day, etc.) and obtains them for fraudulent use.

Assessing fraud risk with mobile

New Customers

- Tell me about this phone number, is it new or tenured?
- Tell me about this device, is it a burner phone?
- Does the user have physical possession of the phone?
- Has there risk that the phone account has been taken over by a fraudster?
- Is there known fraud on this device?

Returning Customers

- Does the phone number still belong to my customer, or has it been recycled?
- Is the device lost or stolen?
- Has my customer upgraded their device since I last interacted with them?
- Has the mobile account been take over via a SIM swap or Line Port?
- Does the user have physical possession of the phone?
- Has there risk that the phone account

Data driven *instant trust* platform

Phone Number Reputation

- Tenure of phone number
- Tenure of mobile account
- Device changes
- Recent port
- Sim changes
- Lost or stolen
- Network suspension
- Post-paid
- Prepaid (cash vs debit)
- Velocity of change events
- Authentication events

Rich data set from SIM-based devices

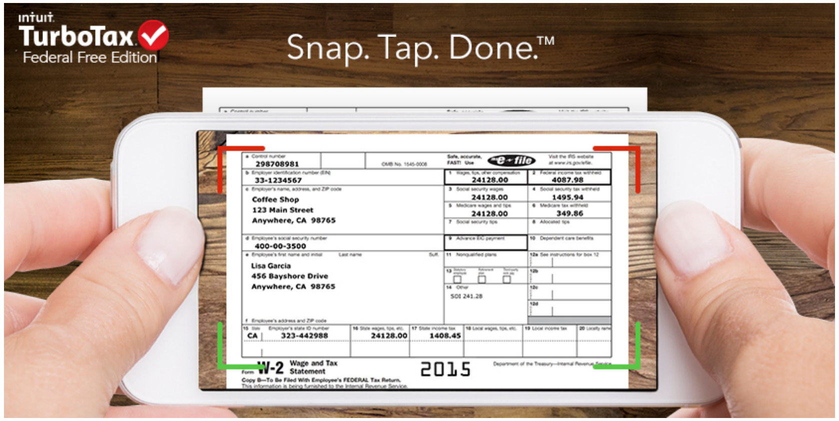
Input Phone number : (917) 555 1212

- Device type = Apple iPhone 6sMNO = AT&T
- Phone number tenure = 420 days
- IMSI = ABC… (globally unique)
- IMEI = A1… (globally unique)
- Master Account
- Post-paid

- Consumer account
- Name = Jill Anderson
- Address = 333 East 91st Street, NY, NY 10128
- Email = jill.anderson@gmail.com
- Phone number history = all prior account ports, phone number changes
- Current location of the device = NY, NY

Mobile Tax Preparation is on the Rise

- 40% TurboTax customers used a mobile device LY
- H&R Block 200% increase from mobile browsers LY
- Ability to use mobile device for authentication and loading of documents such as a driver's license or passport



Source: Fiscal Times

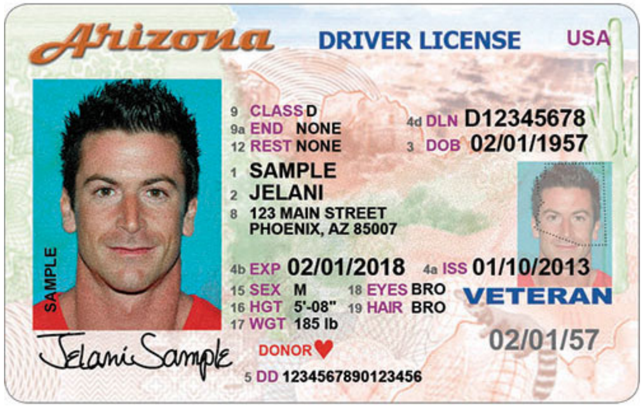
ID Scanning acceptance is increasing

- Provides higher level of verification
- Millennials are a big driver
- Improves user experience
- Faster on mobile devices
- Reduces errors in data entry

Cross-Industry Acceptance

- Financial Institutions – account opening
- Retail – verification for high dollar purchase / returns
- Healthcare – verification for access to health records

Driver's License Structure and info



Arizona DRIVER LICENSE USA

9 CLASS D
9a END NONE
12 REST NONE
1 SAMPLE
2 JELANI
8 123 MAIN STREET
PHOENIX, AZ 85007

4d DLN D12345678
3 DOB 02/01/1957

4b EXP 02/01/2018 4a ISS 01/10/2013
15 SEX M 18 EYES BRO
16 HGT 5'-08" 19 HAIR BRO
17 WGT 185 lb

VETERAN

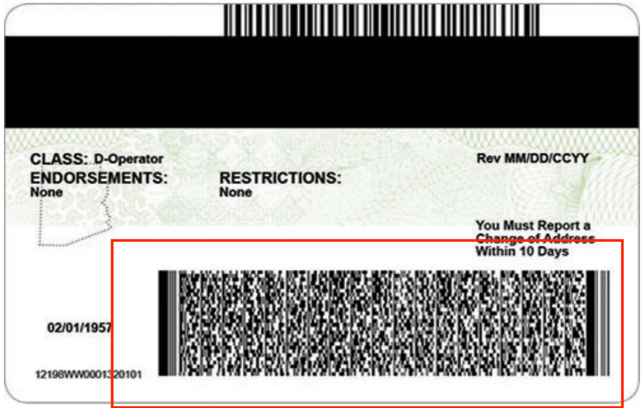
02/01/57

SAMPLE

Jelani Sample

DONOR ♥

5 DD 1234567890123456



CLASS: D-Operator
ENDORSEMENTS:
None

RESTRICTIONS:
None

Rev MM/DD/CCYY

You Must Report a
Change of Address
Within 10 Days

02/01/1957

12198WW0001320101

2D Barcode
w/ info from front

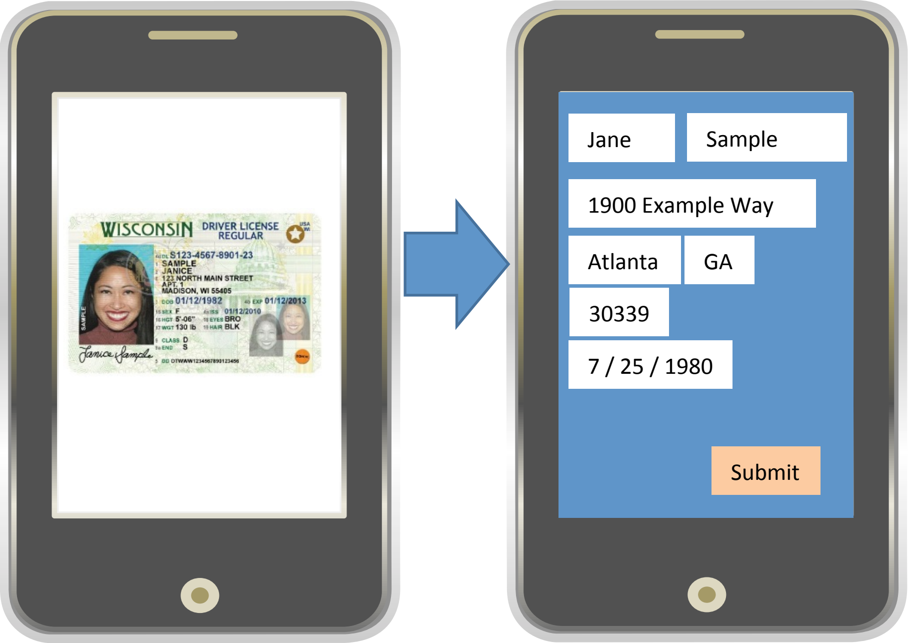
Sample cardholder information
(from front of card)

DL#: 12345678
Last name: SAMPLE
Given names: JELANI
Address: 123 Main Street
City: Phoenix
State: AZ
Zip: 85007
Class: D
Height: 5-08
Weight: 185
Sex: M
Date of Birth: 02-1-1957
Issued: 1-10-2013
Expires: 2-01-2018

DL License Technology Limitations

- Browser-based vs native applications
- Template vs Forensics
- Picture Quality
  - Device Limitations
  - Lighting
  - Bad picture taking

ID Capture & Mobile Devices



Jane
Sample
1900 Example Way
Atlanta
GA
30339
7 / 25 / 1980

- Optimized for mobile devices
- Reduce friction
- Eliminate form abandonment on mobile
- Reduce out of band verifications

- Capture ID with mobile device
- Verify ID
- Extract Data

- Populate forms
- Verify identity credentials
- Escalate when needed

IDology Overview

- IDology is a leading provider of identity and fraud solutions for the tax preparation market – tax preparation and prepaid companies
- Our identity verification and fraud solutions help pass more legitimate returns
  - Issue of the "Perfect Identity"
- Our fraud tools and Collaborative Fraud Network help our customers minimize economic losses from fraud
- IDology's solution today has the tools for US and State government's and private companies to significantly impact the level of fraud and economic loss.

- Our mobile solutions reduce risk via real-time MNO data
  - Mobile Identity
  - Call Center spoofing prevention

- Our ID Scanning Solutions deliver a platform for
  - Verification via ID document scan
  - Step Up authentication
  - Speed up ID review process
  - Reduce fraud