

Why Your New Customer Account Opening Sucks: Build a Robust New Account Opening Experience Without Compromising on Security

A Cautionary Tale: Don't make it too easy for all users



CNN

US

Crime + Justice

Energy + Environment

Extreme Weather

Space + Science

Car sharing service says 100 cars, including 50 Mercedes-Benz, disappeared in Chicago

TOO MUCH FRICTION LEADS TO USER DROPOFF

- Over 50% user dropoff at registration
 - Brand new mobile app with sleek UI
 - Too many fields, specific info
- Asking for Payment info too early in the user registration
 - 60-75% dropoff for retail/ecommerce
- Poor AuthN options
 - 75% of American frustrated with passwords
 - 64% of users refuse SMS OTP

statistics courtesy of: <https://www.ipification.com/blog/how-mobile-apps-can-cut-the-drop-off-rate-in-sign-in-process/>
<https://www.comparitech.com/blog/information-security/password-statistics/>



**Jim
Winters**

Director of Solution Architecture
Transmit Security



**Jake
Lehmann**

Principle Solutions Architect
Transmit Security

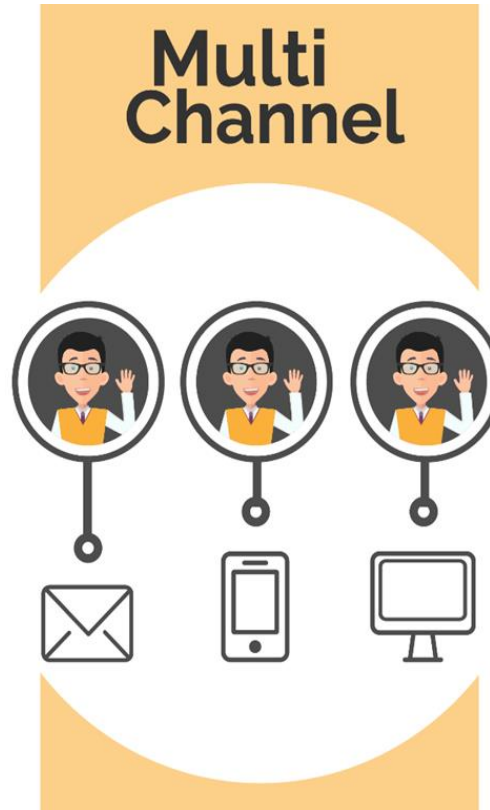
Itinerary

- Challenges
- Best Practices
- Strategies
- Case Studies
- Tools and Technology

Challenges

Challenge: Inconsistent Experience Across Channels

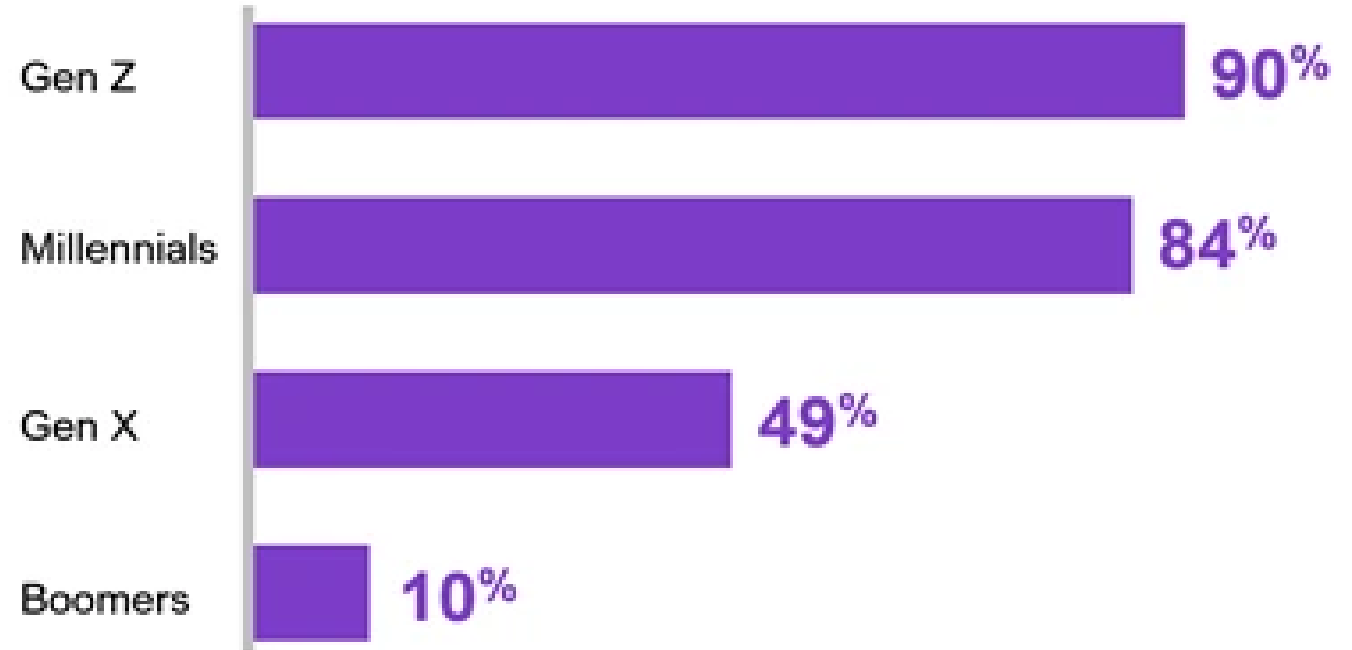
- Web
- Mobile
- In-Person
- Chatbot



Challenge: Lack of Options

- Force in-person interaction
- Users prefer digital channels
- Seamless self service

Digital Service Channels Preferred



Dimension Data 2019 Global Customer Experience Benchmarking: "Which contact channel is most popular with the following age groups?"

Challenge: Internal Use Case

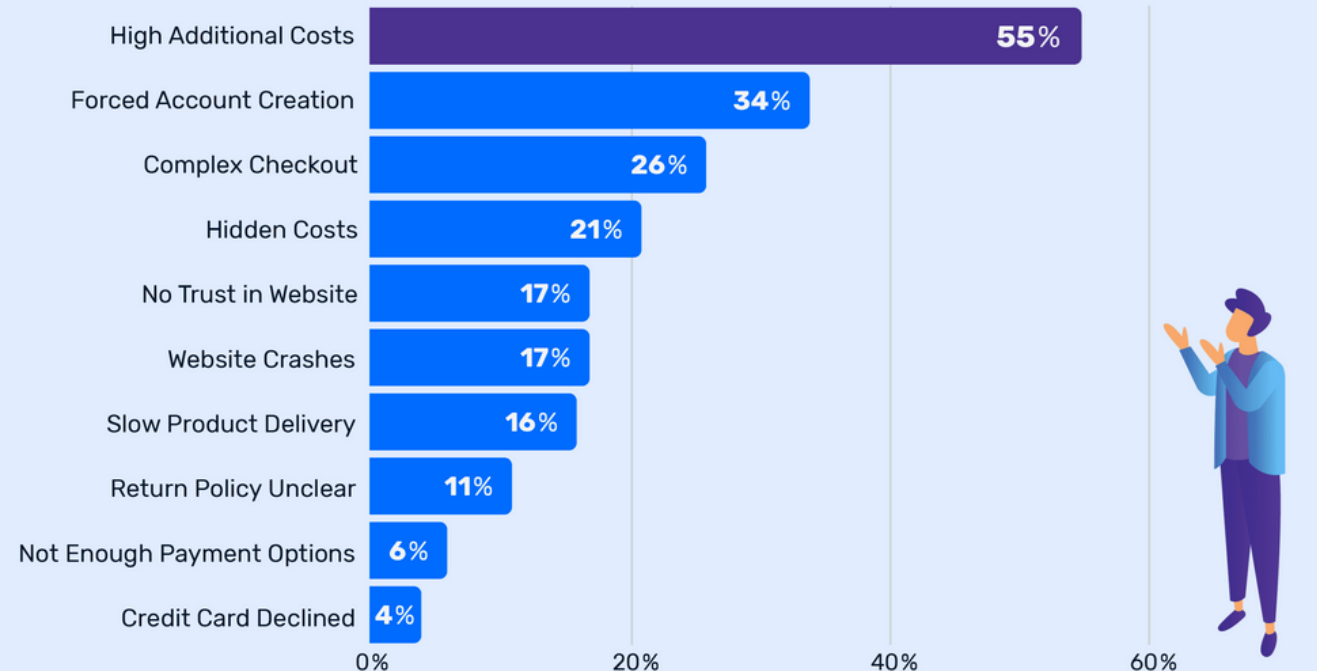
- Partner with business owners
- Understand impact to existing channels
- Know your target audience
- Communicate timing, cost, roadmap



Challenge: User Abandonment

- Balance low friction with enough security
- Drop-off rates often a key business metric
- Allowing guest checkouts

Reasons for Checkout Abandonment



2018: baymard.com/checkout-usability

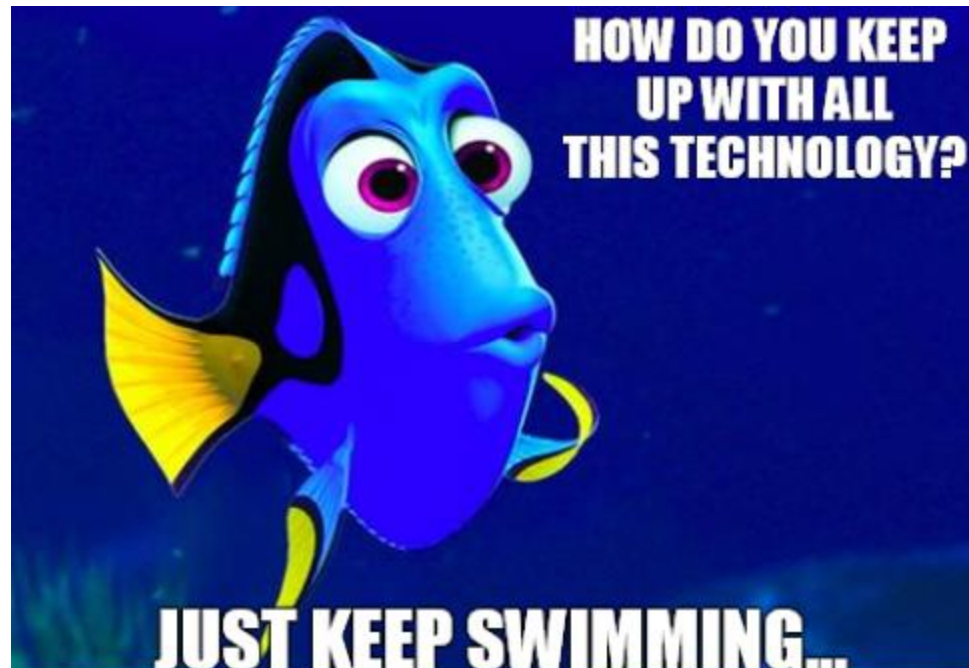
Challenge: Change

- New Use Cases
- New Products
- Pandemics
- Bad Actors
- Data Validation



Challenge: Siloed Solutions

- Point products don't interact
- Best of Breed changes over time
- Different solutions per business group



Challenge: Authentication

- Cumbersome MFA
- Account/password recovery
- Different options per channel

Stock questions

- ✓ What is the food you least liked as a child?
- What is the name of your first stuffed animal?
- What did you earn your first medal or award for?
- What is your favorite security question?
- What is the toy/stuffed animal you liked the most as a kid?
- What was the first computer game you played?
- What is your favorite movie quote?
- What was the mascot of the first sports team you played on?
- What music album or song did you first purchase?
- What is the name of your least favorite child?
- In what year did you abandon your dreams?
- What is the maiden name of your father's mistress?
- At what age did your childhood pet run away?

Manage two-factor authentication

Two-factor authentication is an additional security feature that requires you to use a secondary device every time you log onto *****.

How it works

1. Download the VIP Access mobile app to your mobile device.
2. Launch the app to display the unique Credential ID and six-digit security code.
3. Follow the prompts to link the app to your ***** account.

Challenge: Regulation

- Data Privacy and Protection
- KYC
- Cross-border regulation





















Adult Content

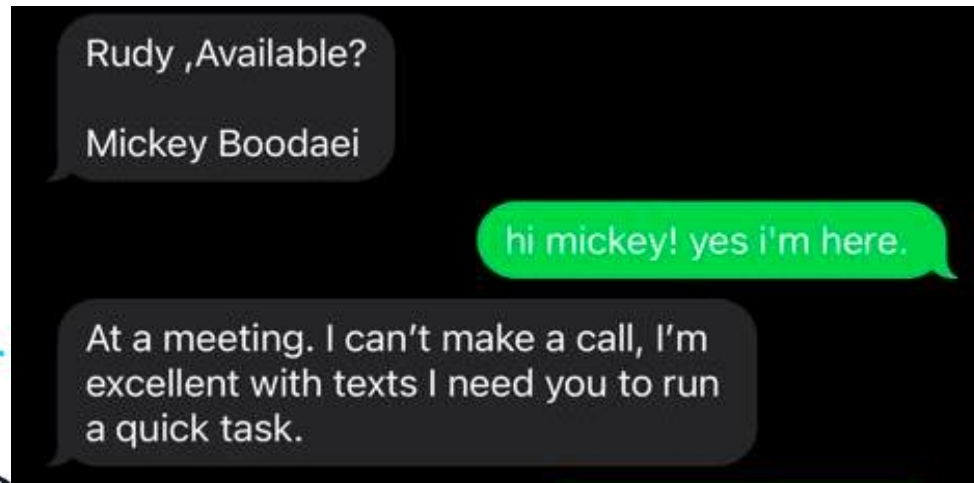
SafeSearch



Challenge: Security

- Data theft is widespread
 - Data validation challenging
- Weak initial validation + weak authentication
- Sophisticated bad actors

671	12,496,605,683	115,743	227,318,427
pwned websites	pwned accounts	pastes	paste accounts
Largest breaches		Recently added breaches	
	772,904,991 Collection #1 accounts		8,227 MEO accounts
	763,117,241 Verifications.io accounts		2,075,625 Terravision accounts
	711,477,622 Onliner Spambot accounts		529,020 OGUsers (2022 breach) accounts
	622,161,052 Data Enrichment Exposure From PDL Customer accounts		400,635 The Kodi Foundation accounts
	593,427,119 Exploit.In accounts		8,000,000 Genesis Market accounts
	509,458,528 Facebook accounts		274,461 Sundry Files accounts
	457,962,538 Anti Public Combo List accounts		114,907 Leaked Reality accounts
	393,430,309 River City Media Spam List accounts		310,975 TheGradCafe accounts
	359,420,698 MySpace accounts		878,290 Shopper+ accounts
	268,765,495 Wattpad accounts		1,658,750 HDB Financial Services accounts

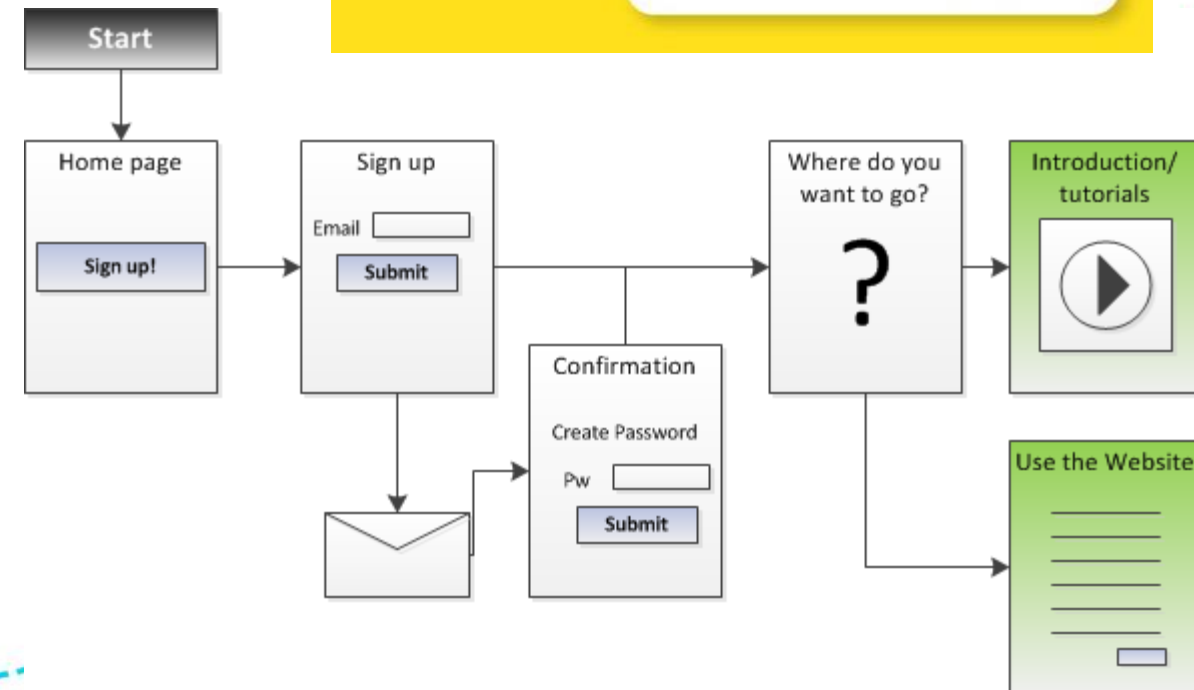
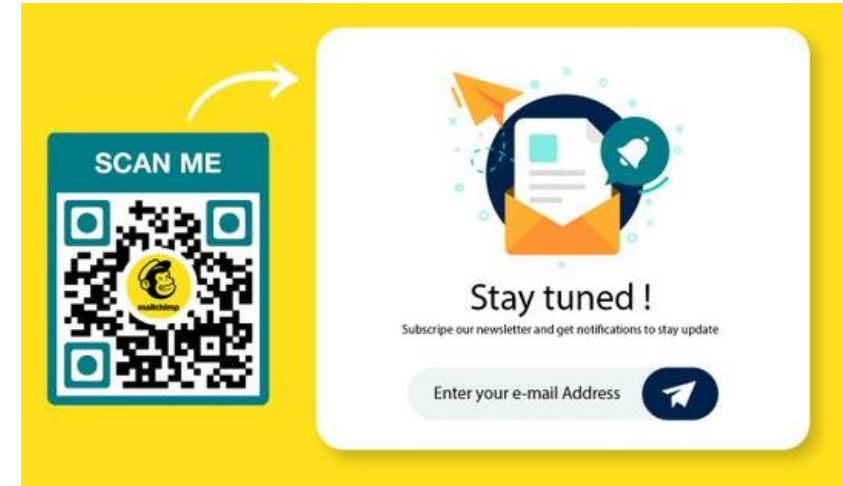


Best Practices

Best Practices: Streamline UX

- Simple is better
- Offer Flexibility
- Educate Users and Provide Support (guided experience)
- Test and Optimize

MIND THE GAP:
Don't overthink this - simple is better

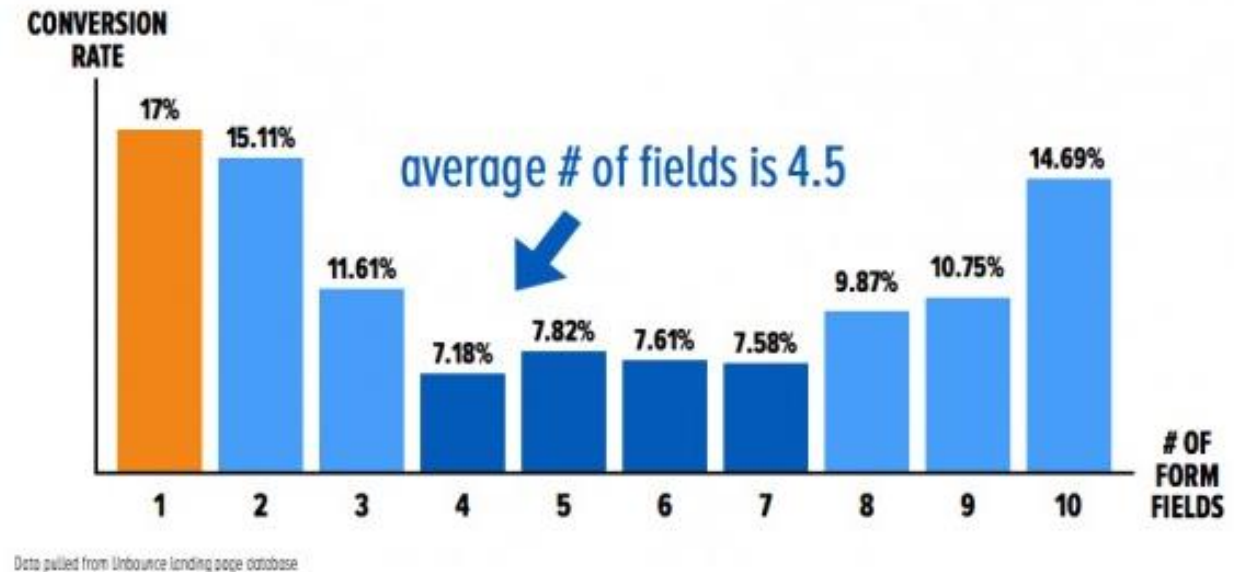


Best Practices: About Those Form Field Statistics

Conversion Rate by Number of Form Fields



Conversion Rate vs. Number of Form Fields



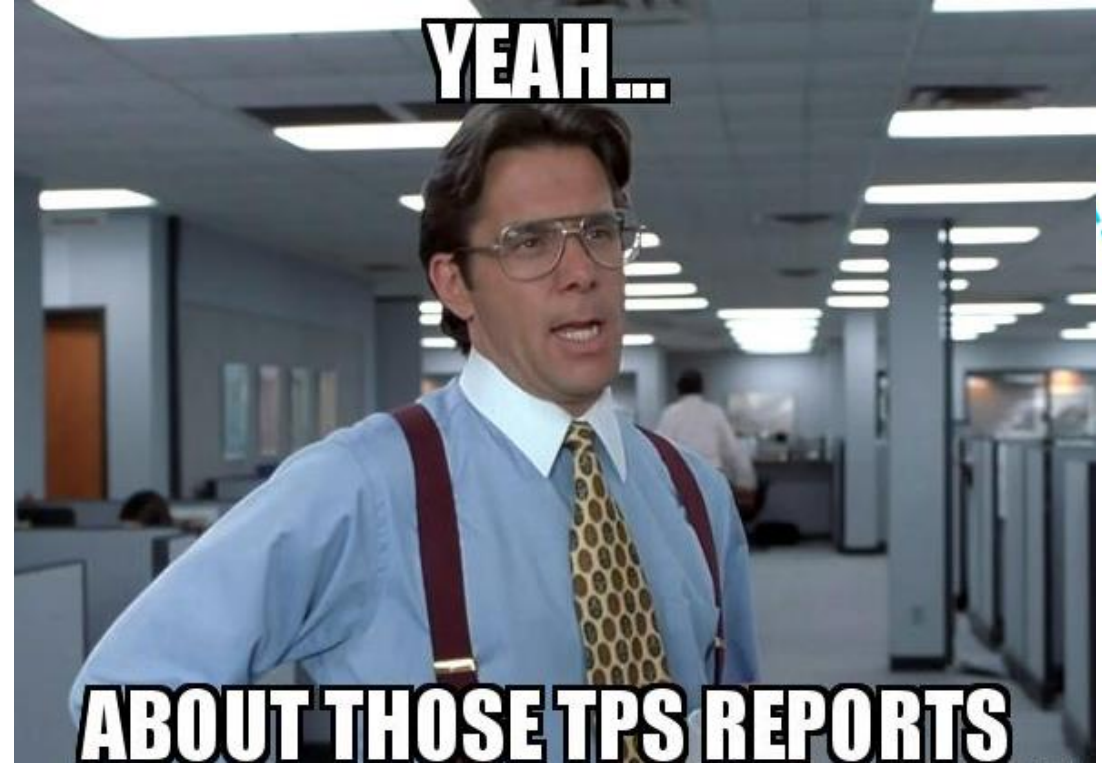
Best Practices: Security

- Strong ID Verification
 - Industry specific
 - Point-in-time specific
- Account for bots
- Strengthen AuthN
 - Multi-factor authentication
 - Biometrics
 - Passive security measures



Business Best Practices

- Ensure Compliance
- Say NO to AI bias
- SLAs
 - Availability
 - RTO
 - RPO
 - multi-cloud
 - Responsiveness and Performance
 - AuthN to your business



Best Practices: Technology Providers

- Partner, not solution provider
- Standards Based
- APIs well documented

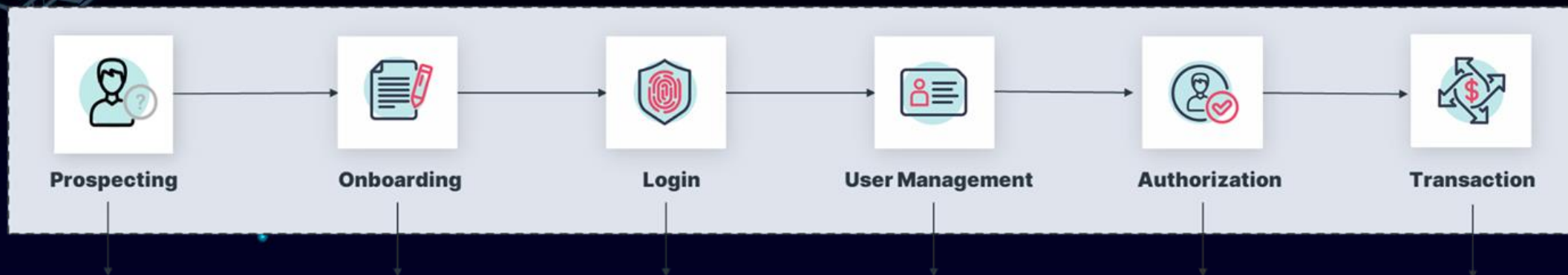


Best Practices: Architecture Concepts

- **“CYBERSECURITY SHOULD BE BAKED IN NOT BOLTED ON”**
- A platform that can orchestrate and/or natively cover all aspects of the consumer identity lifecycle
 - Such as: Onboarding, credentialing, user store(s), authentication, authorization, fraud detection
- Onboarding: Ability to onboard simply, seamlessly, across multiple channels
 - IDV, xDV
- Account Creation and IDM:
 - Scalable & Responsive User Stores
- AuthN: Standards based, passwordless, portable, multi-platform
- Fraud: native or 3rd party risk, trust, fraud, bot and behavior capabilities
- Orchestration
- Ensure your tools can work in harmony

Best Practices: Architecture

Typical identity-related steps implemented by applications



Integration: Multi-Device Developer-Friendly APIs, SDKs, and Low Code



Detection and Response: Risk, Trust, Fraud, Bots, Behavior



Orchestration: Omnichannel Identity Decisioning and Workflows



Identity Verification:
Document Scanning, Data Validation



Authentication:
Passkeys, Passwordless & MFA



Identity Management:
User Profiles, Authorization, SSO

Cloud-Native Architecture





Strategies

Technical Strategies for Maintaining Security in New Account Opening

- Employ Data and Document Verification (industry specific)
- Implement Fraud Detection
- Use MFA, ideally phishing resistant
 - Prevent 99.9% of account compromise attacks!



Business Strategies for Maintaining Security in New Account Opening

- Encrypt & Sign Data (Think CIA)
 - Confidentiality, Integrity, Availability
- Monitor and Audit regularly, stay compliant with regulations
 - Privacy - GDPR, CCPA, etc
 - Industry specific - HIPPA, PCI-DSS, etc
- Train Employees
- Keep User Data Secure



image from nist.gov

Balance Identity Assurance and AuthN Assurance

NIST 800-63b

	Low (level1)	Substantial (level2)	High (level3)
Identity assurance level (IAL)	Self-asserted identity (e.g., email account creation on web), no collection, validation or verification of evidence.	Remote or in-person identity proofing (e.g., provide credential document for physical or backend verification with authoritative source), address verification required, biometric collection optional	In-person (or supervised remote) identity proofing , collection of biometrics and address verification mandatory.
Authentication assurance level (AAL)	At least 1 authentication factor —something you have, know, or are (e.g., password or PIN)	At least 2 authentication factors (e.g., a token with a password or PIN)	At least two different categories of authentication factors and protection against duplication and tampering by attackers with high attack potential (e.g., embed cryptographic key material in tamper-resistant hardware token + PIN, biometrics with liveness detection + PIN/smart card)
Federation Assurance Level (FAL)	Permits the relying party to receive a bearer assertion from an identity provider. The identity provider must sign the assertion using approved cryptography	FAL1 + encryption of assertion using approved cryptography	FAL2 + user to present proof of possession of a cryptographic key reference in the assertion
Level of risk taken by relying party	mitigated	low	minimal

Case Studies

Case Studies: Examples of New Account Opening Experiences

High Friction,
High Assurance

Banks

Insurance

Pharmacy

Travel

Retail

Discord

Low Friction,
Low Assurance

Read a bank case study here:

<https://www.transmitsecurity.com/blog/leading-us-bank-achieves-1300-roi-with-transmit-security>

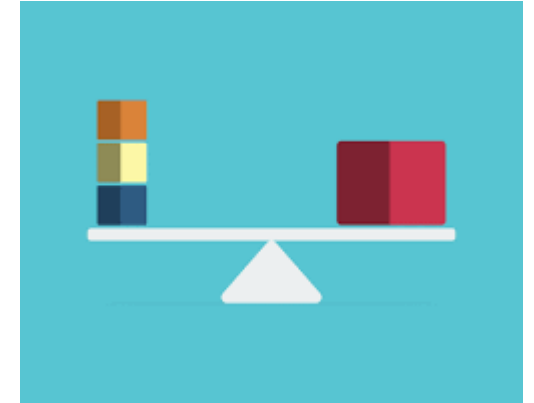


#identiverse

Tools and Technologies

Balancing Friction and Security

- Use strong ID proofing only when necessary
 - Post-account creation
 - At checkout
 - When fraud signals indicate risk
- Risk and Fraud tools without user interaction
- Layered approach to security to prevent synthetic account creation and bad actors



I Know It's You, Now What

- Match AuthN to User Journey
 - Step up when needed
- FIDO2 phishing resistant credentials
- Seamless experience for trusted users



Registration and AuthN UI Delivery Options

- Build It - fully customizable
 - API
 - SDK
- Hosted - some customization
- OIDC/SAML - someone else's customization

Access Citi.com With QR Code

Sign on to Citi.com with Citi Mobile® App, instead of your User ID and password, for enhanced security.

Note: Only customers who are enrolled in Face ID®, Touch ID®, Biometrics or 6-Digit PIN are eligible to sign on using QR Code.

Here's How It Works:

Step 1

Open Citi Mobile® App and select QR Code* from the Sign On screen.

*Can also go to: Profile > Security Center > Citi® Trusted Identity



Step 2

Hold your phone steady on the QR Code. Once in focus, it will automatically scan the QR Code.



Step 3

When the QR Code is scanned, you'll be signed on to Citi.com.



Scan this QR code using your Citi Mobile® App



QR Code refreshes every 45 seconds. After the third refresh, click Sign On With QR Code to generate a new code.

Welcome back!

We're so excited to see you again!


EMAIL OR PHONE NUMBER *

PASSWORD *

[Forgot your password?](#)

[Log In](#)

Need an account? [Register](#)

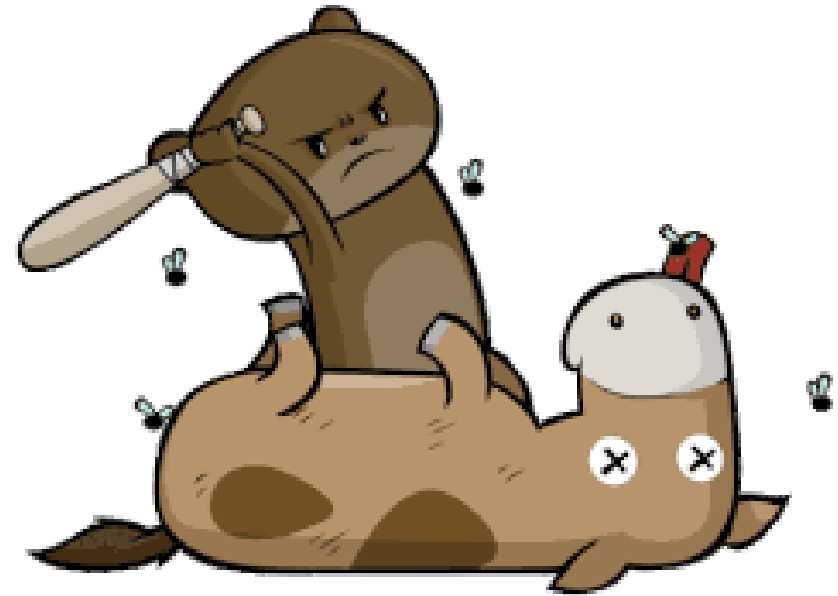


Log in with QR Code

Scan this with the Discord mobile app to log in instantly.

Keep Our Data Safe

- End to End Encryption
- Secure Data Store
 - Still using passwords? Salt and Modern Hashing, please
 - Use opaque identifiers where available
- Ensure your vendor is secure
- Decouple Identity and Authentication



Conclusion

Conclusion

- **Cybersecurity, Fraud, ID Proofing, Authentication, Privacy —> Are NOW CIAM**
 - Gone are the days of a provider that focused just on joiner, mover, leaver
- Think NOT about tech first, but about the user journey
 - Mindful of UX
- You (probably) can't do it all - so look for a provider that can augment your identity-security capabilities
 - Invest in a Responsive and scalable User Store



THANK YOU!