AShield

Anything else
is a compromise.

Leading you into a Future with **High Trust** and **Minimal Fraud**

A Decade Apart – The Shifting Landscape of Authentication

2006

2024

Dynamic form of authentication	Extremely vulnerable
Cost effective	Highly expensive today
Easy to use	Negligible security
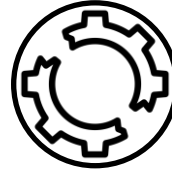
AShield

Anything else
is a compromise.

OTP is vulnerable at all stages of its lifecycle

At SMS delivery partner

- Twilio, Syniverse systems breached – OTP leaked
- OTPs hijacked via cheap partner subscriptions

Man-in-the-middle Attack

SS7 flaws in telecom enables OTP interception by fraudsters – Crypto Frauds

Entered from Hacker's device through

Phishing, Vishing, and free virtual numbers bypass OTP

At Mobile Device

Auto-forwarding malware installed on user's device - forwards OTP codes

Existing solutions have outlived their utility

Point Solutions – Lack of continuous verification

Purely Predictive Solutions – Leads to false positives and false negatives

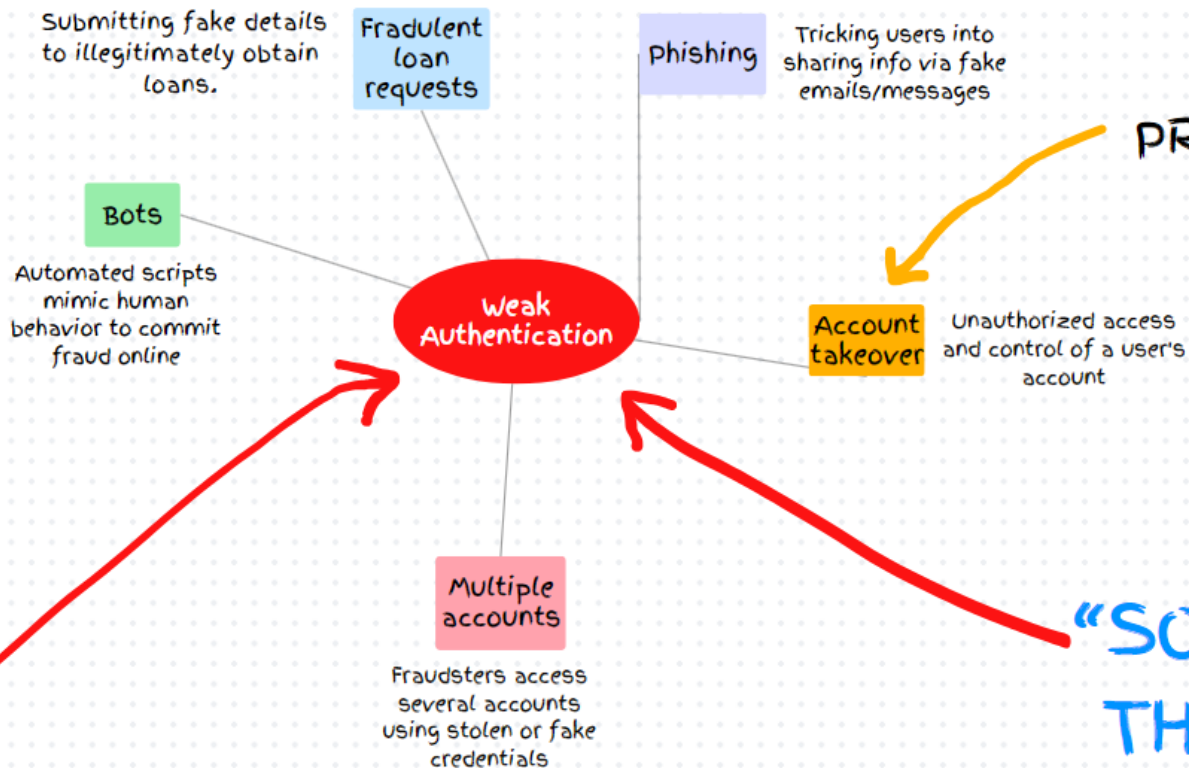**Phishable Solutions –** Authenticators, OTP codes are phished easily

Weak Device Binding

We provide Enterprises with **a Cost-effective 1-click** User Verification Solution of the **Highest Security** with **Uninterrupted Customer Experience**.
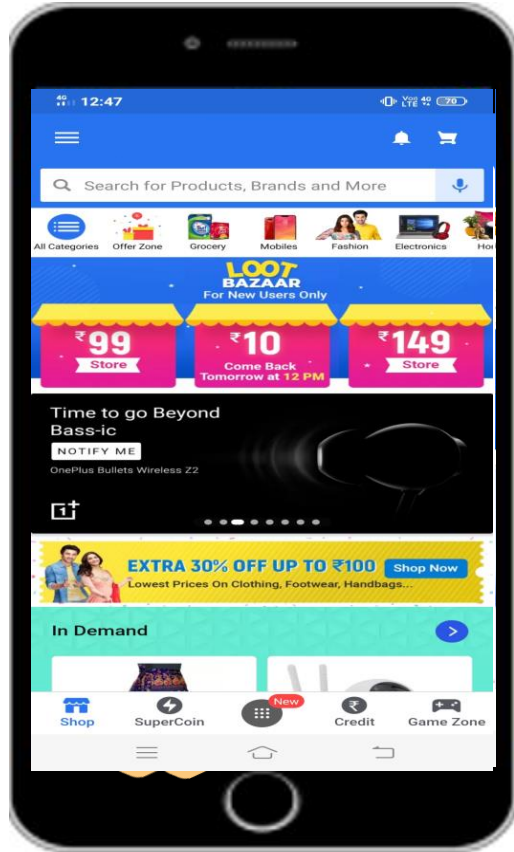
Mobile App Login Before **A**Shield

User clicks on Login

User Types in his/her 10-digit Mobile Number and clicks 'Continue'

6-digit OTP is sent to User. User has to additionally key it in, and then click 'Continue'

User is successfully logged in, on successful verification of OTP, after **18+ clicks**

Limitations of OTP Login before AShield:

➤ Multiple clicks, crippling **Customer Experience.**

➤Extremely prone to **Phishing attacks**. OTPs have been compromised at all stages in their lifecycle.

➤OTPs have an average User Drop-off Rate of **18-24%.**

➤OTPs can be intercepted for as little as **$16**.

Mobile App Login After **A**Shield
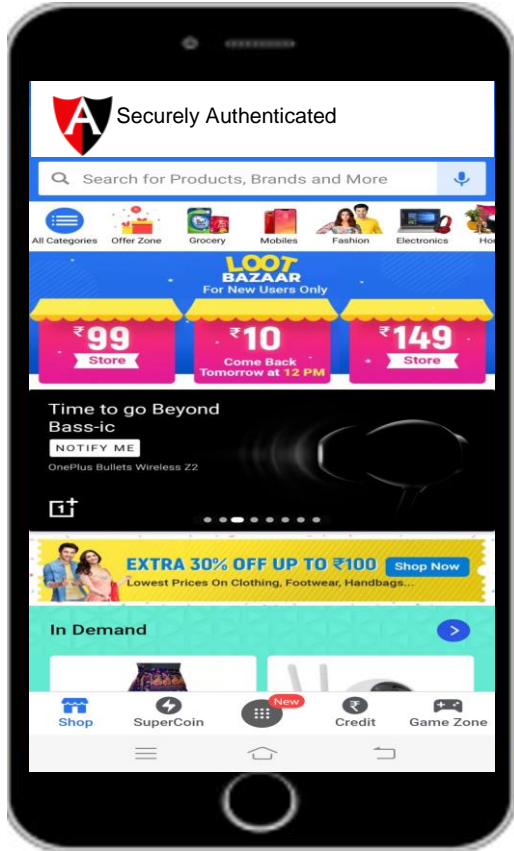
User clicks on 'Login'

User is **Securely Authenticated** in just **1-Click**

OS-based Passkey verification (FIDO)

Login Benefits After AShield:

➢ One-Touch Rapid Login with **Top-Notch Security., enhancing CX.**

➢ The only truly **Phishing-proof** user verification solution.

➢ Leverages **OS-level encryption bound to Enterprise domains,** preventing fraudulent access if device is stolen.

➢ Provides **Continuous Security** throughout user journey.

➢ **Active SIM Presence & Device Fingerprint** is detected at every step.

Browser login before **A**Shield

AShield
Anything else
is a compromise.
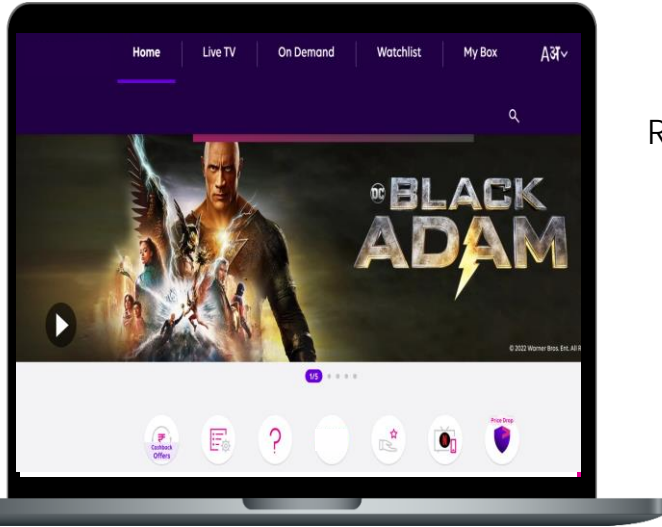
User only needs to enter Registered Mobile number and OTP for verification

OTPs alone provide insufficient security for account access

Limitations before AShield:

- OTPs are powerless against advanced threats and are phishing-prone.

- Every time the user comes in, they have to enter the Mobile number and OTP, crippling CX.

- Increasing user drop-off on the platform.

First time Browser login after AShield
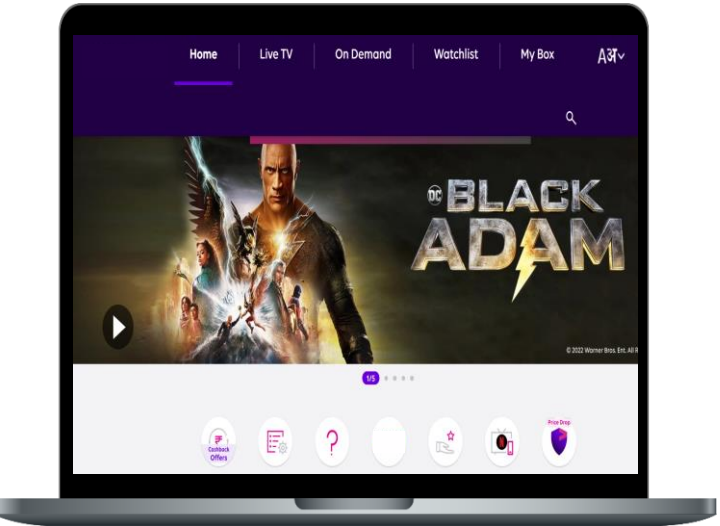
The User enters Mobile Number & OTP ONCE for user verification

OS-based Passkey verification (FIDO)

Enterprise Server

- Highly secure Crypto shares are created and distributed for further authentications.

- AShield keeps one Crypto share, while the other 2 are stored with Enterprise and the device

- OS-level Encryption bound to Enterprise domains leveraged for subsequent seamless access

Subsequent Browser logins after **AShield**
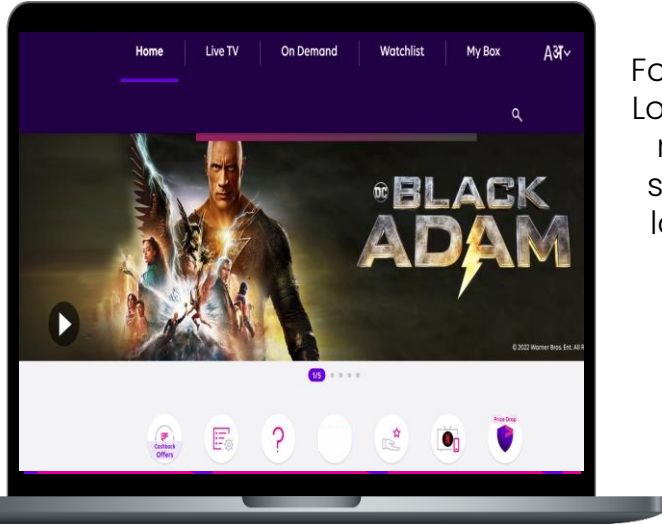
Enterprise Server

For subsequent Logins, the user needs just a single click to log in to their account

- Crypto shares are validated.
- User is successfully authenticated.
- Old shares are destroyed.
- New shares are created and distributed.

Benefits after AShield:

- Seamless perpetual Login experience for the users.

- Ultimately helps in saving OTP cost.

- Can be used to seamlessly secure user verification in other business critical areas.

- User input for OS-level passkey verification, triggered optionally, for secure device binding.

Wallet transactions before **AShield – Prone to fraud**

AShield
Anything else is a compromise.
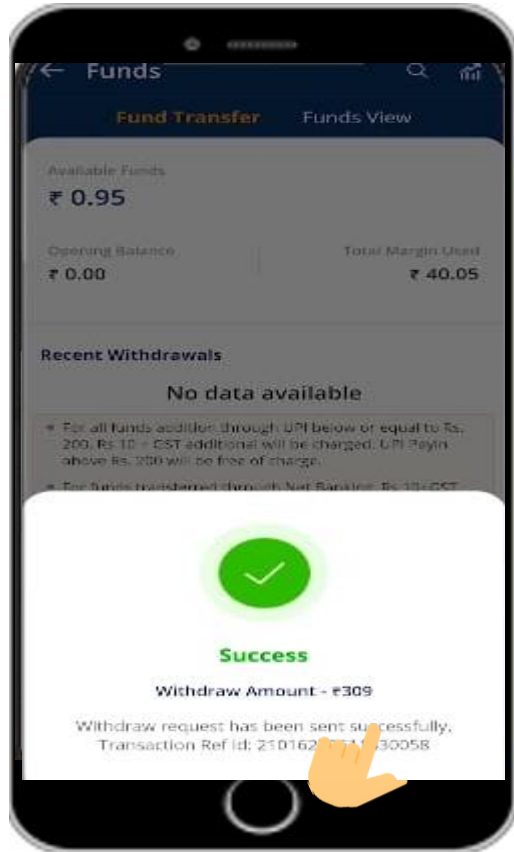
Post ATO, fraudsters initiate fraudulent money requests and withdrawals

With no user verification process here, financial fraud takes place

Limitation before AShield:

- Post account takeover, fraudsters can initiate false money requests.

- **No mode of authentication** to prevent fraudsters from generating fraudulent transactions.

- Any mode of authentication introduced will be phished and reduce conversions.

Secure Wallets with AShield
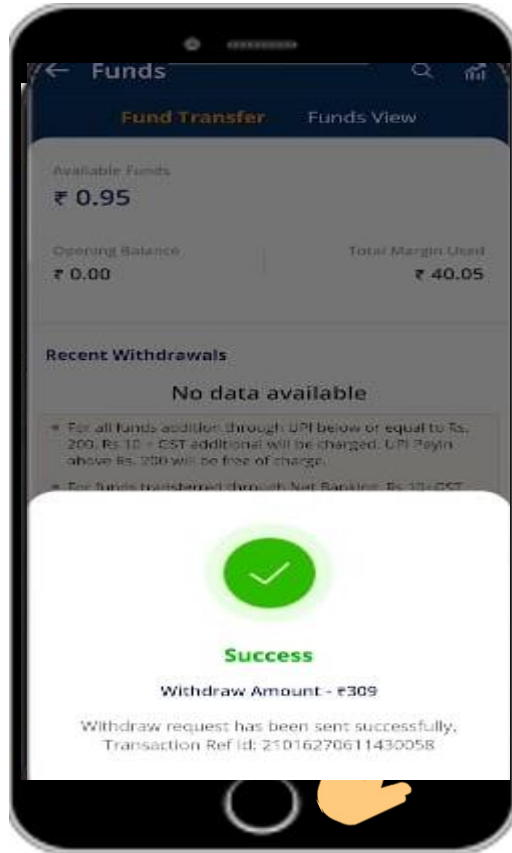
Only legitimate users can initiate money transferring requests

User is Securely Authenticated in the background with No additional Click
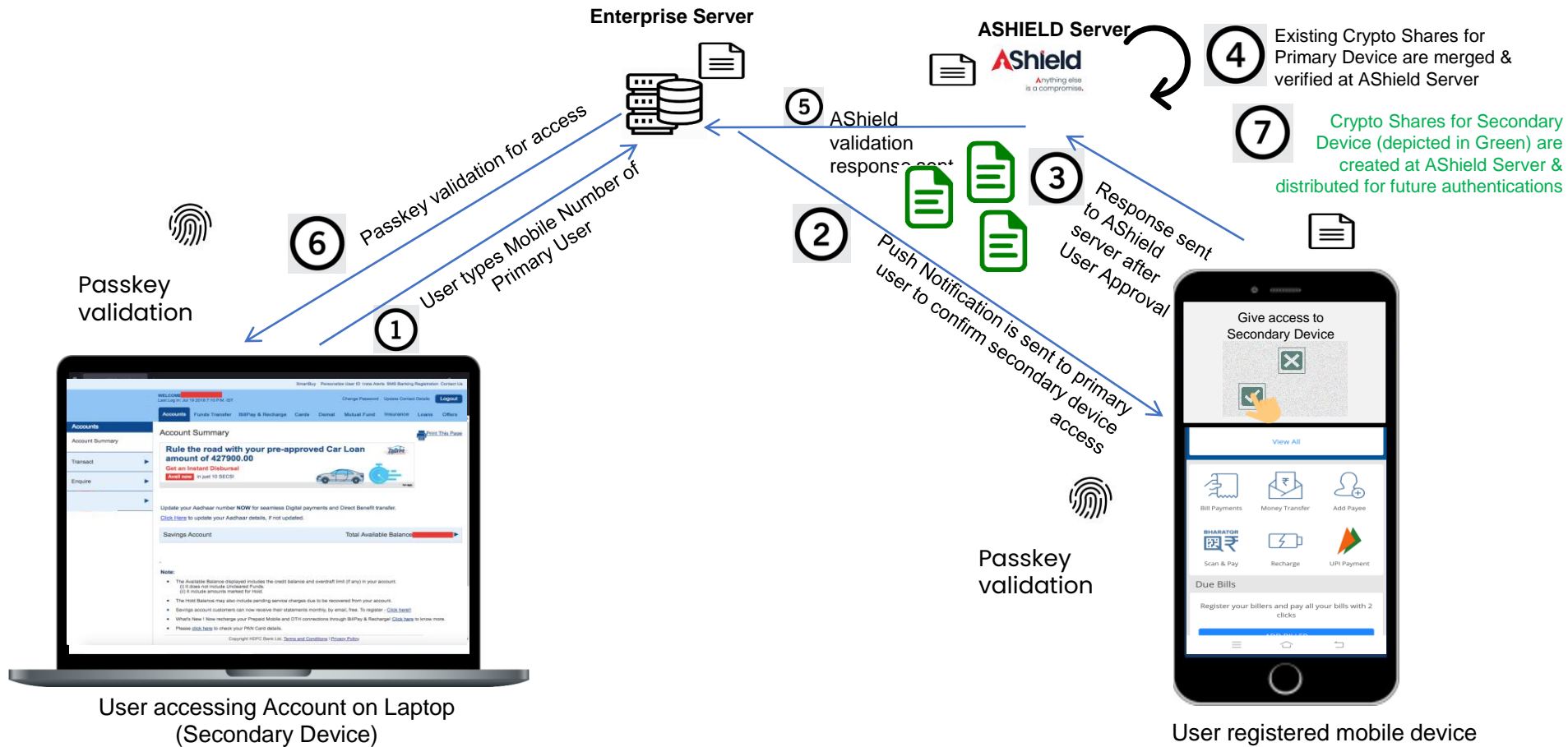

OS-based Passkey verification (FIDO, triggered optionally)

Benefits after AShield:

- Genuine users will be able to transfer money after secure verification that happens in the background without hampering current CX

- Best Security is achieved with no change in the current process.

- User input for OS-level passkey verification triggered optionally for device binding.

AShield Secured Multi Device Access

Enterprise Server

ASHIELD Server

AShield
Anything else
is a compromise.

④ Existing Crypto Shares for Primary Device are merged & verified at AShield Server

⑦ Crypto Shares for Secondary Device (depicted in Green) are created at AShield Server & distributed for future authentications

⑤ AShield validation response sent

③ Response sent to AShield server after User Approval

② Push Notification is sent to primary device user to confirm secondary device access

Passkey validation for access

⑥

① User types Mobile Number of Primary User

Passkey validation

Passkey validation

Give access to Secondary Device

View All

Bill Payments   Money Transfer   Add Payee

Scan & Pay   Recharge   UPI Payment

Due Bills

Register your billers and pay all your bills with 2 clicks

User accessing Account on Laptop (Secondary Device)

User registered mobile device

AShield: Revolutionizing Security for Bajaj Finserv

Bajaj Finserv, one of India's leading fintech giants, struggled with fraudulent activities including fake accounts and account takeovers, affecting customer trust and operational efficiency.

Solution: AShield introduced a seamless one-click authentication solution, eliminating traditional OTP methods that were exploited by fraudsters. This innovative approach not only closed the gateway for fraudulent activities but also enhanced customer experience by reducing friction

Impact:

- **Customer Experience**: Improved journey by minimizing friction.

- **Cost Savings**: 20% reduction in SMS costs.

- **Transaction Success**: Over 300 million successful transactions.

- **Fraud Prevention**: Blocked 60 million fraudulent attempts.

AShield's innovative solution ensures security and user-friendliness, protecting Bajaj Finserv's extensive user base while optimizing costs.

The undeniable value of **undoing** OTPs & Passwords

2.8 BILLION+
Live Commercial
Transactions Processed

2 Beta Customers in the US

AShield – Against the Point Solutions of OTPs and Password. A Superior Comprehensive Solution that drives down the cost.

AShield
Anything else
is a compromise.

Insulated from Imposters

through

One-Touch Sign-In and Securing Every Customer Transactions

AShield Technologies Pte. Ltd.

Corporate Headquarters: 30 Cecil Street #19-08 Prudential Tower Singapore 049712

Enquiries: yrsuccess@ashield.co

ashield.co