Early Warning®

EARLY WARNING MOBILE SECURITY SUITE

Achieving Out-of-Band Mobile Authentication

Evolution of Mobile Interactions

Mobile devices have become an extension of the consumer, usually always "on" and accessible, creating a close relationship between the individual and device. With innovation and adoption of mobile wallets in addition to mobile banking and merchant payment apps, consumers are using their mobile devices in two very distinct ways:

- Mobile as a proxy for identity / factor of authentication
- Mobile as a channel to carry out transactions

As mobile interaction methods continue to evolve and grow, organizations are increasingly challenged to deliver a seamless consumer experience while ensuring the safety and soundness of the transaction.

INTEGRATING WITH MOBILE NETWORK OPERATORS

Early Warning brings together three critical categories to help organizations solve the mobile authentication challenge. By coupling the consumer's mobile phone number and device hardware with real-time connectivity to the Mobile Network Operators (MNO), organizations can better ensure they are interacting with the right customer.

Leveraging the same SIM-card based network authentication that the mobile carriers use to secure their own services, Early Warning's suite of Mobile Security Solutions enables organizations to gain an unprecedented level of identity and device confidence, far surpassing traditional and device-centric measures.

EARLY WARNING MOBILE IDENTIFIER

By verifying customer identity, mobile device and account ownership at the carrier level, a true 1:1 unique authentication bind known as the Early Warning Mobile Identifier is established.

The Early Warning Mobile Identifier serves as a persistent key that can't be manipulated and stays with the consumer regardless of mobile changes. Common customer events such as managing lost or stolen phones, changing carriers and phone number reassignments can also be managed in real-time without disturbing the customer.

With the Early Warning Mobile Identifier at the core, the device hardware is queried in real-time to determine the status of the device and account and looks for any recent changes that may have occurred. This provides an Out-of-Band, network authenticated solution that includes the ability to revoke, or trust the device when accessing secure systems.

Only Early Warning can deliver this unmatched level of mobile authentication as well as the most current and accurate financial transaction and identity data. Now, organizations can authenticate mobile accounts and devices with greater confidence to better mitigate fraud, manage risk and create a seamless experience for the consumer.

EARLY WARNING DIFFERENCE

Only Early Warning Works In Device Hardware (e.g. SIM Card)

Other Mobile Auth Solutions Work Here (e.g. App Download)

Mobile Network Operator

The Mobile Security Suite of solutions answer three distinct questions:

1 MOBILE AUTHENTICATION: WHO ARE YOU INTERACTING WITH IN REAL-TIME?

Mobile Authentication validates the mobile device accessing the mobile app or mobile browser and acts as a secure Out-of-Band Authentication (OOBA), two factor authentication from a trusted 3rd party (MNO). By authenticating a consumer's mobile number and device with the MNO, organizations gain a higher degree of confidence that the consumer on the mobile device is the true customer.

BENEFITS

- Gain confidence that the consumer on the mobile device is the true customer
- Confirm customer relationship with device and carrier for mobile app and mobile browser use cases
- Garner a secure Out-of-Band Authentication, two-factor authentication from a trusted 3rd party (MNO)

2 MOBILE STATUS: HAS ANYTHING CHANGED SINCE THE LAST INTERACTION?

Mobile Status monitors for changes in the device as well as mobile account information. It ensures the device status is valid and has the potential to identify possible risky transactions. Mobile Status provides the following:

FEATURES

- Mobile ID created date
- Account role
- Customer type
- Account type
- Network status
- Change events (with dates)

BENEFITS

- Know the age of an account
- Determine account role of device user — Owner, Member, Employee
- Determine if device is under a personal or business account
- Verify if account is pre-paid or post-paid
- Verify if the account is active, deactivated or suspended
- Identify risk change indicators (SIM swap, new number, new device, etc.)

3 MOBILE IDENTITY: IS THE PERSON AUTHORIZED ON BEHALF OF THE MOBILE ACCOUNT?

Account ownership of the device is validated based on details provided by the customer to their operator. A match/no-match score is returned as part of the process to confirm details on file with the MNO.

- Matching score — Name and Address
- Verify, flag your CRM info on file
- Optional matching score — Email
- Returns "Exact Match," "High Match," "Conditional Match," or "No Match" results

For more information about Mobile Security Suite, contact an Early Warning Account Manager at earlywarning.com/auth.

ABOUT EARLY WARNING

Early Warning Services, LLC, is a fintech company owned by seven of the country's largest banks. For almost three decades, our identity, authentication and payment solutions have been empowering financial institutions to make confident decisions, enable payments and mitigate fraud. Today, Early Warning is best known as the owner and operator of the Zelle Network®, a financial services network focused on transforming payment experiences. The combination of Early Warning's risk and payment solutions enable the financial services industry to move money fast, safe and easy, so people can live their best financial lives.

To learn more about Early Warning, visit www.earlywarning.com