Early Warning®

FORTIFIED OTP: SECURING THE DELIVERY OF ONE TIME PASSCODES

Authentication for a Passwordless Customer Experience

Businesses often rely on SMS messages as a way to authenticate a transaction by validating a consumer is in possession of a trusted device. While this has been the standard, specific vulnerabilities and shortcomings have been acknowledged. Criminals are tech-savvy and have discovered ways to take advantage of this process by intercepting, forwarding or replicating SMS messages on another device, making fraud much harder to detect. Because of this, this type of scheme is lucrative for thieves to conduct social engineering attacks to forward an SMS to another device or to even intercept the SMS code to gain unauthorized access to accounts.

Concerned about the lack of controls around SMS as a stand-alone authentication mechanism, in 2016 the National Institute of Standards and Technology (NIST) discouraged companies from using SMS based authentication in their two-factor authentication schemes.[1] Despite their vulnerabilities, the reliance on SMS two-factor authentication was too great, and in 2017 NIST backed off their initial position.[2] Today, given the guidance of security experts, the primary tool is to utilize One Time Passcodes (OTPs) via SMS to authenticate consumers in addition to various other authentication methods.

In addition to organizations reliance on OTPs, consumers have become accustomed to using an SMS authentication passcode as well. However, usernames and passwords will eventually become security theater as financial institutions (FIs) will be able to authenticate the consumer with behind the scenes authenticators. Regardless, authentication via a mobile device will not go away anytime soon and banks must be able to send verified, secure messages to the intended recipient to authenticate customers without the use of cumbersome passwords or passcodes.

KEY BENEFITS

Enhance security of SMS and passive authentication

Improve the customer experience by reducing friction

Authenticate customers without the use of cumbersome passwords

Protect against social engineering attacks, SMS forwarding, SMS scraping and man-in-the-middle attacks

Sources:
1 National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Lifecycle Management. Dec, 2016.
2 National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Lifecycle Management. Jun, 2017.

Improving the Customer Experience

Now, businesses can utilize out-of-band authentication to validate that the intended device received a passwordless, secure message. By utilizing Early Warning's Fortified OTP solution, banks can utilize either active or passive authentication to validate consumers:

FORTIFIED OTP

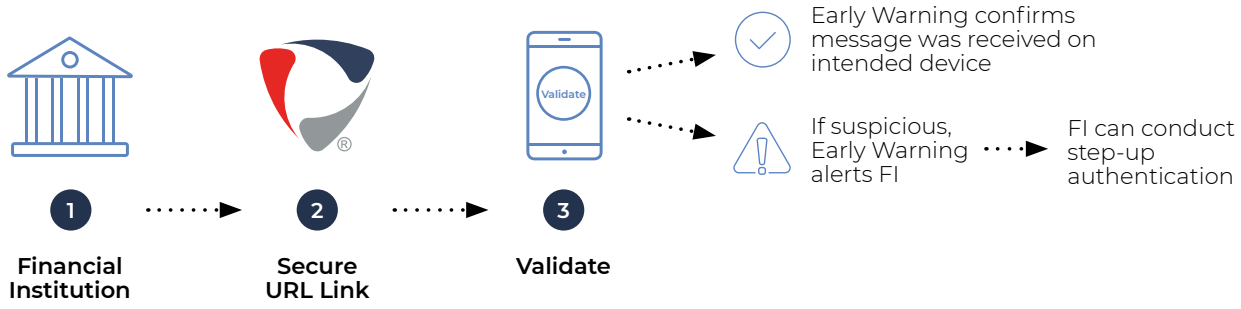
A customized SMS can be sent with a secure URL link to authenticate a consumer with the touch of a link on their mobile phone and without the hassle of a password. This enhanced security allows for a better customer experience while providing a second factor token to authenticate the user and validating that the SMS has made it to the intended mobile number/device. Another option is to send an 800 phone number to the recipient to confirm receipt of the OTP and that the text made it to the right device.

SILENT OTP SECURE MESSAGING

In order to bolster secure messaging functionality, Early Warning's Silent OTP solution can be embedded within your mobile app or texted to the consumer for seamless, silent authentication. By utilizing Mobile Network Operator (MNO) data through Early Warning, we can passively determine if the message was received on the anticipated device or if step-up authentication should be utilized. It enables the use of a trusted device to login to an account, eliminating the need for Knowledge Based Authentication while overcoming the deprecation concerns of OTPs.

How It Works

Early Warning utilizes information directly from the MNOs to identify the customer and associate them to the right mobile device and account via the secure hardware-based revocable token (e.g., SIM card). This creates a one-to-one unique authentication bind that is created to form a persistent identifier for each transaction — whether initiated online or through a mobile network.



To schedule a demo of this solution, contact an Early Warning Account Manager at webinquiry@earlywarning.com.

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