AllClear ID

AllClear CrossChannel™

Transform Your App to Remove Friction in Every Part of your Business

Friction Intolerance v. Security

Mobile technology and apps have fundamentally changed what qualifies as a friction-free experience. Customers are sold on mobile conveniences like biometrics, and they are becoming intolerant of journeys that require passwords to access accounts, phone calls to authorize important actions and standing in line to pick up orders.

Mobile first organizations are taking full advantage of the powerful devices their customers carry 24/7 while companies that operate web sites, retail locations and call centers are stuck with the old ways of doing things.

Meanwhile, cybersecurity threats and regulations compound friction in every channel—including mobile. Recently, mortgage banks and title companies were forced to take a giant step backwards due to massive escrow scams. Now they wave red security flags and encourage buyers to hand deliver cashier's checks to make escrow payments. Even mobile-first organizations are forced to restrict app functionality because they can't fully trust the customer's device.

Organizations are caught in a vice with friction intolerance on one arm and security requirements on the other. Customers are left wondering why they can't use their mobile devices to do everything.

Savvy organizations are responding by transforming their mobile app into a cross-channel tool that removes obstacles and unleashes innovation no matter where, how or when customers engage.

For example:

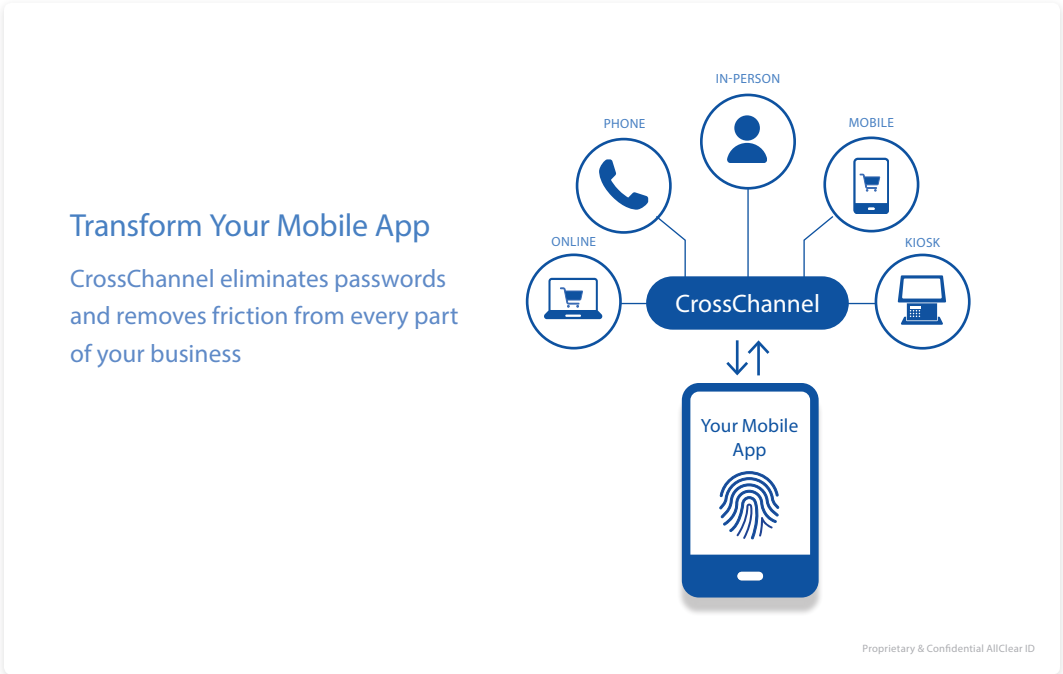
- Instead of relying on passwords and security questions, they are inviting customers to use their mobile app to access website and call center services with the touch of a finger. They are eliminating passwords entirely—not simply using biometrics to autofill passwords on the device.
- Rather than using email or third-party services to acquire signatures, organizations send documents directly to the mobile app for biometric signature.
- Rather than asking customers to wait in line to pick up online orders, the mobile app signals the customer's arrival time and location so that associates can greet them with their order in hand.
- Instead of restricting app functionality because of security risks, they are implementing protections that keep their app safe from mobile threats and man-in-the-middle attacks.

This white paper describes a transformative platform that makes these experiences possible and highly secure.

Introducing the AllClear CrossChannel™ Platform

CrossChannel is a cloud-based platform that connects your mobile app to every part of your business. The idea is simple. Give customers the convenience, speed and security of mobile and connect it to all customer facing channels; website, in-store, call centers, mobile and kiosk. The result is a customer experience that is faster and more secure by design.

ILLUSTRATION 1:



CrossChannel's In-App Automations are the key to bringing mobile technology to every service channel.

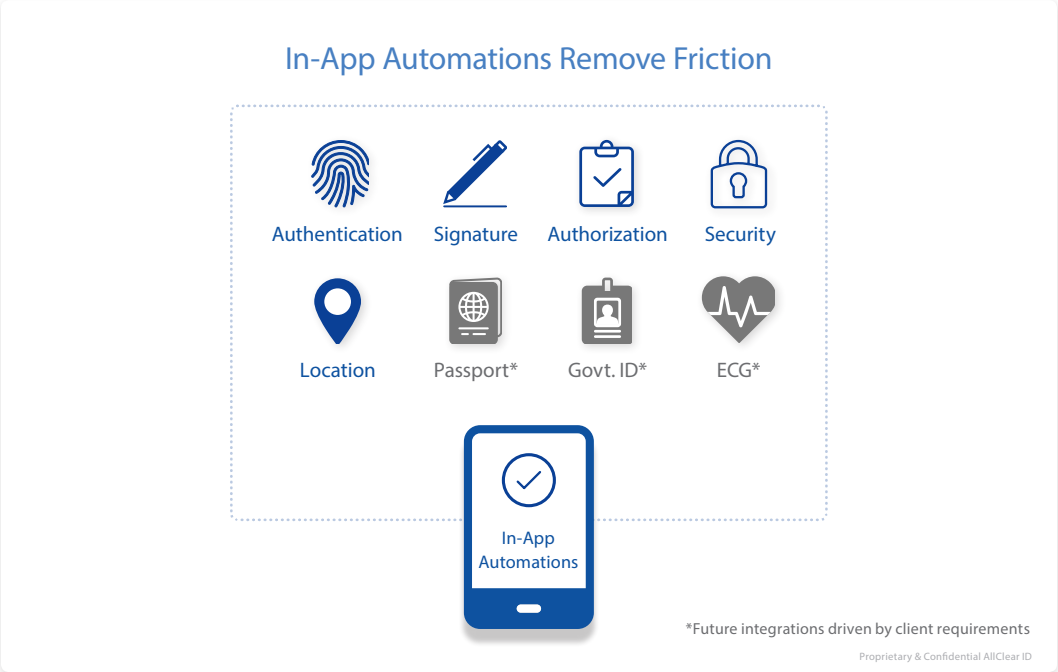
- **In-App Authentication replaces passwords:** Now customers can use their fingerprint or face to authenticate in every service channel. No more passwords or security questions.
- **In-App Signatures eliminate delays:** Rather than using a scanner or third-party service to sign documents, customers can instantly sign documents using their mobile biometrics.
- **In-App Authorization reduces phone calls:** Instead of requiring phone calls, email or in-person meetings to authorize important actions, enable in-app authorization with context, biometric authentication and electronic audit trails.
- **In-App Location speeds logistics:** Bring the power of GPS to every channel to verify location and accelerate service or product delivery.
- **In-App Security unleashes features:** Banking grade security protects apps from mobile threats so that you can release high value features with confidence.

The cost of one password related support call is $70, and a large percentage of support calls are related to passwords.[1]

Source: Forrester Research

Approximately 30% of online purchases are abandoned at checkout because consumers cannot remember their passwords.[2]

ILLUSTRATION 2:



Patented and Proven

CrossChannel is banking grade technology that accelerates over 345 million financial transactions every year for banks, retailers and airlines. The core engine, Encap, is a third-generation product that is highly configurable and runs reliably on over 2 million iOS and Android devices. No scalable attacks have been reported since its introduction in 2012, and the core technology is certified to meet the world's highest banking standard for authentication, Secure Customer Authentication (SCA).

[1] https://searchenterprisedesktop.techtarget.com/tip/Resetting-passwords-in-the-enterprise-without-the-help-desk

[2] https://www.thenational.ae/business/up-to-11-hours-spent-every-year-resetting-passwords-1.819620

The CrossChannel Platform:

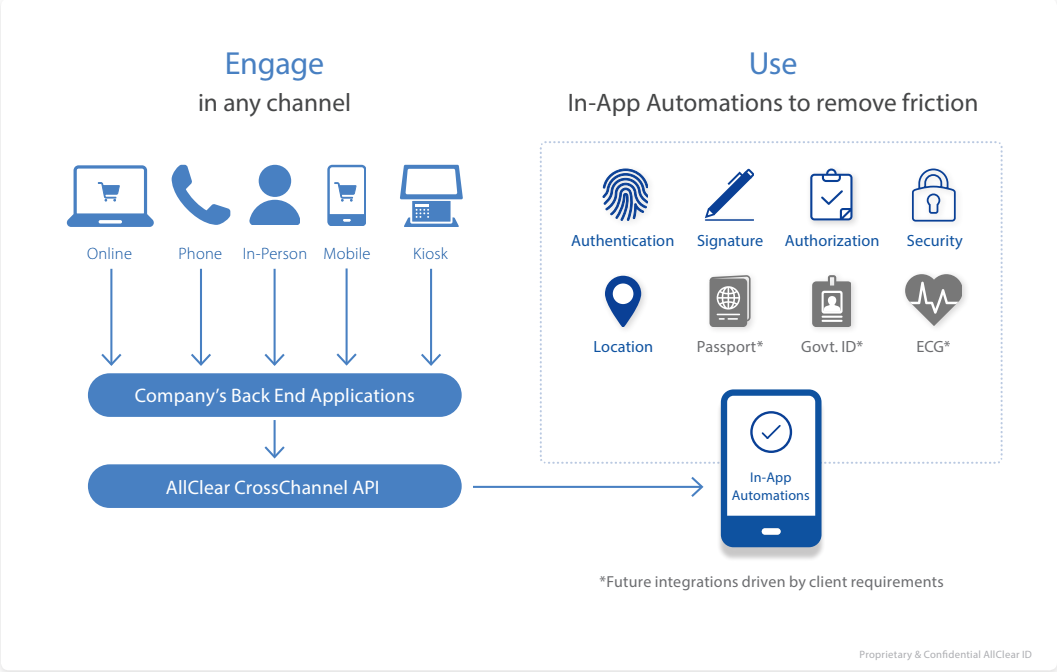
- Radically reduces friction in every part of your business
- Unleashes innovation with In-App Automations
- Increases customer engagement by up to 300%
- Keeps systems safe with proven banking grade security

How it Works

The CrossChannel solution consists of two components: the CrossChannel API that integrates into back-end applications, and the Mobile Software Development Kit (SDK) that embeds In-App Automations in the mobile app. These components establish a two-way, high security communication channel between the organization's back-end applications and the customer's mobile device. The communication channel is designed to transmit any data, images or other content in both directions.

Whenever mobile technology can improve a step in the customer journey, the back-end application pushes the action to the customer's device to accelerate the process. The push message launches the organization's mobile app which presents the context and action to the customer. Upon completion, it returns the result and any requested data to the back-end application.

ILLUSTRATION 3: HOW CROSSCHANNEL WORKS



More Secure by Design

The CrossChannel technology was originally designed for mobile-first banks in the Nordics. The central challenge was to safely execute any banking operation on mobile devices and computers that the banks could neither control nor trust. The mobile app was the key, and it needed to be protected even when operating on a compromised platform. The resulting design has proven highly resistant to phishing, malware, man-in-the-middle and other malicious attacks that plague other systems.

First, the design "short circuits" attacks on front-end applications by crossing channels to complete steps using the customer's mobile device. To succeed, attackers must steal the customer's mobile device and overcome multiple security factors (physical device, fingerprint, face, PIN and location). It blocks the front-end attacks that plague password-based systems including:

- Password Theft and Re-use
- Social Engineering
- Friendly Fraud (via non-repudiation)

Second, it blocks man-in-the-middle attacks with forward-secret cryptography that dynamically generates keys within the Trusted Platform Module (TPM) on the device. The TPM is an isolated hardware component designed to keep cryptographic operations secure even when the operating system kernel is compromised.

Third, the CrossChannel Protocol and Mobile SDK combine to block mobile attacks including:

- Device Cloning
- SIM Swapping
- Mobile Malware
- App Debugging
- App Repackaging
- App Emulation

The core technology is certified to meet the world's highest banking standard for authentication, Secure Customer Authentication (SCA). This new standard is defined under Payment Services Directive 2 (PSD2), and no longer permits multi-factor authentication solutions like texting one-time passcodes.

Some startling facts around password usage:

81% of people reuse the same password across multiple accounts[3]

29% of people share passwords with two or more people[3]

People often rotate the same set of passwords or simply add a digit to them to make them "unique"

The most common password is "123456" followed by "Password"[4]

[3] https://www.keepersecurity.com/assets/pdf/Keeper-Mobile-Survey-Infographic.pdf

[4] http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

Use Cases

The technology limitations in different channels serve up a "friction cocktail" that confounds customers holding superior technology in their hand. In home buying for example, customers scout properties using mobile apps, sign contracts using email, apply for mortgages using websites and complete the journey at a conference table with an ink pen. Along the way, they have to remember the passwords for each app and website, repeat answers to security questions and sometimes dust off a fax machine to get the job done.

CrossChannel lets customers use the power of their mobile devices to remove all this friction. Following are a few use cases.

- **Financial Services/Customer Authentication:** A new home buyer wishes to fund an escrow account from their online savings account. The buyer accesses the online savings account by entering his or her phone number into the bank's website and uses the bank's mobile app and their fingerprint to authenticate. The buyer uses bill pay to set up the payment and escrow recipient. After submitting the bill for payment, the bank pushes the payment instructions and signature request to the mobile app for final confirmation and biometric signature.
- **Healthcare/Call Center Services:** A member has a question about a recent bill and calls their health plan's 1–800 Member Support line. Instead of interrogating the member with security questions, the IVR invites the customer to authenticate using their mobile app while waiting on hold. The customer enters their mobile number and instantly receives a push message that opens their mobile app and prompts them for their fingerprint. The IVR confirms their identity and connects them caller to an agent for service without the interrogation. The member requests their medical records be transferred to a new plan. The agent pushes an authorization request form to the mobile app. The member enters the receiving plan information and signs the authorization request with their finger.
- **Retail/Online Purchase with Curbside Pickup:** A customer purchased an item from the service provider's website and elected to pick it up from the store later that same day. One hour prior to the pick-up time, the retailer pushes an offer to meet them curbside when they arrive. The customer taps the push message to open the app and consents to the retailer using their location to anticipate their actual arrival time for faster service. The request asks for the make and model of their vehicle and offers add-on purchases with the touch of a finger. Upon arrival, the store dispatches an associate to greet the customer at the curb with the order in hand. If the order is valuable or regulated, the customer receives an authentication request after the vehicle is parked and the associate is cleared to hand over the goods.

In each of these examples, the customer stays inside the trusted brand experience with CrossChannel removing friction and securing the journey.

Conclusion:

Mobile technologies have reduced the amount of friction that customers will tolerate, and the technologies used to conduct business in other service channels seem antiquated by comparison. Separately, cyber security requirements are compounding friction and forcing organizations to limit functionality in every channel.

The AllClear CrossChannel platform addresses this dilemma by transforming mobile apps into cross-channel tools that remove obstacles from every part of a business. This innovative approach has been proven in Nordic countries (see history below) where mobile banking apps are fully functional and highly secure. Now CrossChannel is making this technology accessible and affordable for every industry.

The History Behind CrossChannel

Nordic countries have long been leaders in mobile technology and digital identity solutions. They built the world's most widely adopted digital identity ecosystem used daily by 21 million people to access accounts, make payments and engage government services. The roots of this identity design began in 1999 with Norway's BankID scheme that used physical tokens such as key fobs for banking customer authentication.

Sweden began laying plans for their e-ID scheme in 2001, also deploying physical identity tokens. Denmark and Finland soon followed suit, and now all four countries utilize a banking identification scheme that ensures strong consumer identity. Over the past few years, all have matured and strengthened their original authentication designs moving from key fobs to the use of SIM cards to now deploying state-of-the-art app-based solutions using the customers preferred hardware, mobile devices.

Leading the app-based research was Encap AS which started inside the Bank ID project. Encap was eventually spun out to develop a commercial product, and in 2016, Encap and Bank ID demonstrated the convenience and security of the app-based model. Now the entire ecosystem is moving to the app-based model. In 2016 AllClear ID acquired Encap and continued advancing the technology to solve friction problems well beyond authentication. In late 2019, AllClear ID released a SaaS version of the product named CrossChannel. It is powered by the Encap engine, and its purpose is to make this powerful technology accessible and affordable to every industry around the world.

About AllClear ID

AllClear ID, Inc. pioneered the cross-channel technology that allows application builders to use the power of mobile devices to radically reduce friction in any part of their business. The core engine, Encap, features banking grade technology that accelerates over 345 million financial transactions every year for banks, retailers and airlines. It is a proven, third-generation product that is certified to meet the world's highest authentication standard, Secure Customer Authentication (SCA).

The award winning AllClear ID team is also recognized for its identity protection products, high quality service and successful deployment of large-scale managed services. AllClear helped organizations like Anthem Blue Cross, Home Depot and Sony to respond successfully to data breaches affecting 200 million customers. Experian acquired the breach response business from AllClear ID in March of 2019, and the company is now focused exclusively on the CrossChannel/Encap product line.

For more information about AllClear ID and AllClear CrossChannel solution

contact: www.allclearid.com or call 1.877.441.3007