



Ping & Fingerprint

Joint solution brief





Introduction

eCommerce fraud is on the rise, with online payment fraud losses globally estimated at \$41 billion in 2022 and projected to reach \$48 billion in 2023. The surge in eCommerce fraud is primarily due to the increase in online shopping brought about by the COVID-19 pandemic, allowing fraudsters to exploit the eCommerce industry.

Moreover, eCommerce stores are grappling with another issue — cart abandonment. Statistics from 2022 revealed that 71% of online shoppers abandon their carts before purchasing due to user friction, leading to an approximate loss of \$18 billion in sales annually.

Balancing user experience and security measures by implementing an identity solution that powers frictionless and secure customer experiences is crucial in addressing these challenges.

Overview of Ping & Fingerprint

Ping Identity – Identity and access management leader

Ping Identity, an industry leader in identity and access management (IAM), helps you protect your users and every digital interaction they have while making experiences frictionless. Digital experience is a competitive advantage but multiple identity systems often become a roadblock. PingOne DaVinci's no-code orchestration allows you to design seamless and secure user experiences across your entire technology ecosystem. If you can whiteboard it, you can orchestrate it.

With PingOne DaVinci, you can: integrate your entire identity tech stack, regardless of the vendor; design your user journeys easily, reducing dependency on developers; and easily test and make changes to optimize the user journey.



Fingerprint – Device identification leader

Fingerprint helps catch sophisticated fraudsters and personalize experiences for trusted users with our 99.5% accurate device intelligence platform. Our technology combines hundreds of signals inside any browser or mobile application to generate a unique identifier to understand visitor behavior better. Unlike traditional device identification platforms, Fingerprint provides additional device intelligence that is easily implemented into existing fraud models and decision engines.

Fingerprint offers two commercially developed capabilities:

- **Identification signals.** The most accurate browser fingerprinting service available. Instead of relying solely on cookies or IP addresses, Fingerprint combines an array of 100+ unique signals that can identify users with a 99.5% accuracy for every user touchpoint.
- **Smart Signals.** Smart Signals provide enhanced actionable intelligence around user behavior, bot detection, and network signals including incognito mode, IP geolocation, VPN browser tamper detection, and more to help you make faster, more-informed decisions about your traffic.

Joint solution overview

As leaders in IAM and device identification, Fingerprint and Ping Identity have partnered to provide a seamless and secure user experience, leveraging the PingOne DaVinci no-code identity orchestration service. Fingerprint allows PingOne DaVinci customers to reduce fraud by integrating the most highly accurate device identification and intelligence into their DaVinci user journeys.

Together, Fingerprint and Ping provide an accurate device identification solution that is quick to deploy and provides immediate value to end customers.

Accurate

Accurate 99.5% and future-proofed stable visitor IDs that last for months instead of days

Fast deployment

Quickly implement and integrate with pre-built connector and workflows to easily start identifying devices right away

Immediate value

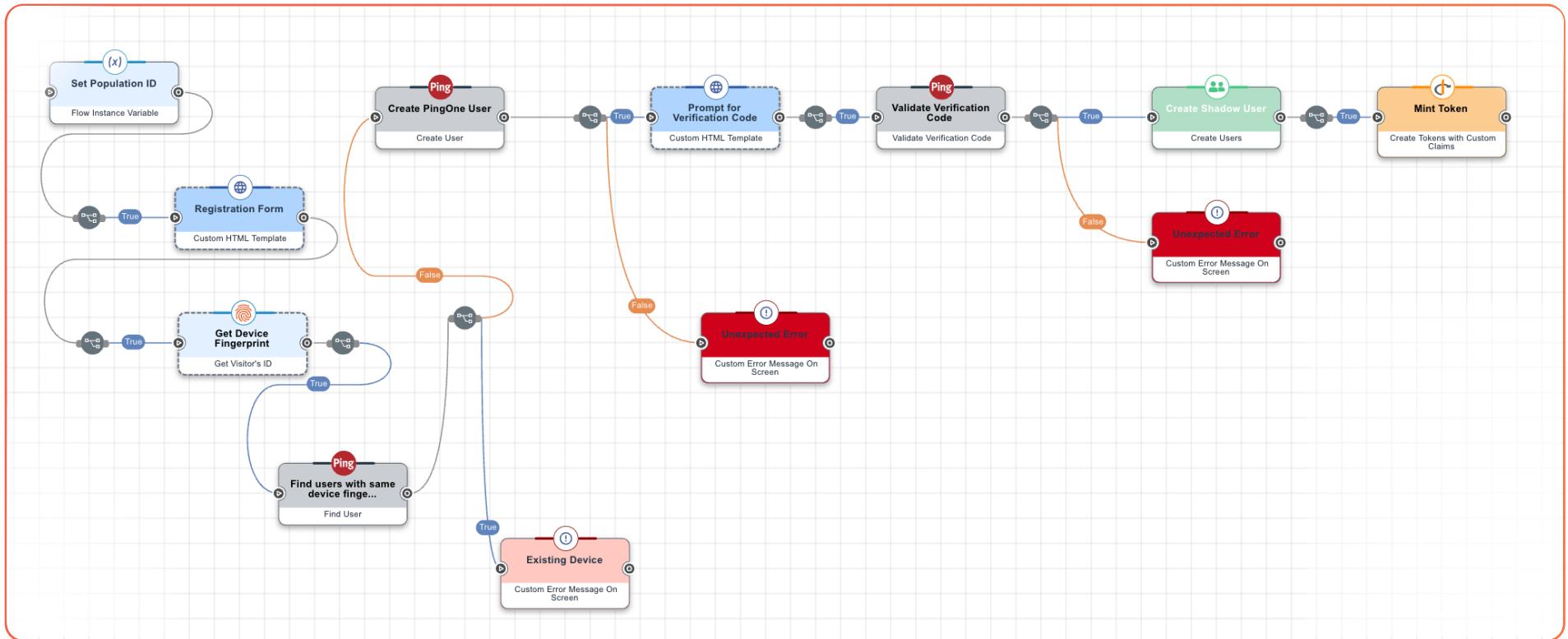
Automated flows optimize end user experience at every stage of the customer journey while maintaining security and reducing fraud



Specific use cases

Fingerprint can be easily embedded into various user flows using PingOne DaVinci to reduce fraud and improve the user experience.

One example is **registration flow**, which can also be known as new user registration or account sign-up. You can add a Fingerprint visitor ID to a new user profile. And you can also prevent visitor IDs with more than a certain number of accounts to create a new account to stop free-trial abuse.

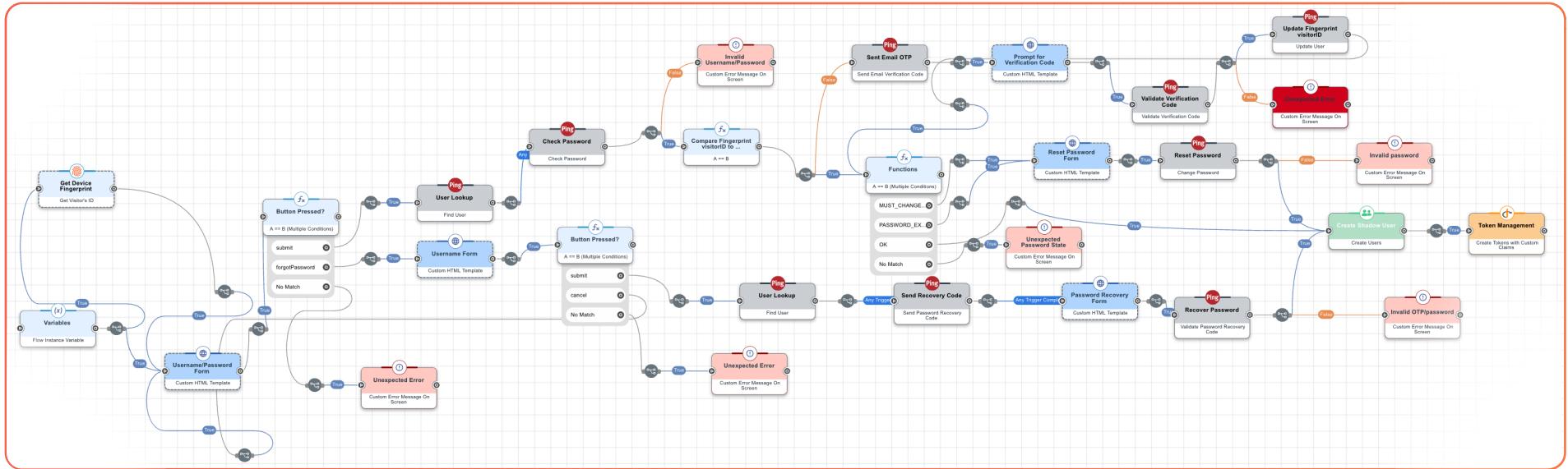


Registration flow explained...

1. Users create new accounts within Ping.
2. Ping calls out to Fingerprint to get the visitor ID.
3. Optional – Check if the visitor ID exists in other user profiles.
Block registration if it does for more than X users.
4. Fingerprint device ID is stored in PingOne.
5. New account is created and associated with the device.



Another use case for Fingerprint embedded in PingOne DaVinci is a **risk-based authentication flow**, which helps prevent account takeover and maintain account security. This is an important flow as it prevents bad users from resetting an account password and stops login attempts from flagged devices.



Risk-based authentication flow explained...

1. User logs in on a PingOne-controlled webpage.
2. Fingerprint API generates a visitor ID.
3. User enters credentials.
4. PingOne DaVinci orchestrates the flow to look up user information.
5. If credential check passes, then look up visitor ID for that user to verify if it matches the current one (passive MFA).
6. If user information and visitor ID match, then there's no need to step up to second factor authentication.
7. If user information and visitor ID do not match, then step up with PingOne MFA.



Summary

Fingerprint and PingOne DaVinci provide a highly accurate and future-proofed device identification solution that is quick to deploy and provides immediate value to end customers. With Fingerprint and Ping, you can reduce fraud while delivering seamless and secure user experiences.

Get started with the [PingOne DaVinci Fingerprint Connector](#) today to reduce fraud and improve the user experience at every stage of the customer journey, from account sign-up to risk-based authentication sign-on and payment transactions.

About Ping Identity

At Ping Identity, we believe in making digital experiences both secure and seamless for all users, without compromise. That's digital freedom. We let enterprises combine our best-in-class identity solutions with third-party services they already use to remove passwords, prevent fraud, support Zero Trust, or anything in between. This can be accomplished through a simple drag-and-drop canvas. That's why more than half of the Fortune 100 choose Ping Identity to protect digital interactions from their users while making experiences frictionless.

Learn more at www.pingidentity.com.

About Fingerprint

Fingerprint, powered by the most accurate device fingerprinting technology, enables companies to prevent fraud and improve user experiences. Fingerprint processes almost 100 signals from the browser, device, and network to generate a stable and persistent unique visitor ID that can be used to understand visitor behavior. With a commitment to best-in-class data security and privacy, Fingerprint is proud to be ISO 27001 certified, SOC 2 Type II, GDPR, and CCPA compliant. Fingerprint is trusted by over 6,000 companies worldwide, including 16% of the top 500 websites, to help catch sophisticated fraudsters and personalize experiences for trusted users.

Learn more at www.fingerprint.com

