Solution Brief

Prevent Fraud, Reduce Risks with Real-time, Multi-layer, Seamless Identity Verification & Authentication

Zumigo solutions leverage multiple real-time, deterministic signals that represent a consumer's different identity artifacts to verify their identity, preventing fraudulent activities across the digital engagement journey without adding friction.

To protect the network perimeter from identity-related vulnerabilities, and counter escalating identity fraud risks like Account Takeover (ATO) and synthetic identity, businesses need a multi-layered identity verification and authentication framework that is seamless to the consumer and accurate in the risk analysis.

Zumigo provides the essential intelligence layer to this identity-first security framework by leveraging multiple real-time, deterministic signals from mobile network operators (MNOs) and other digital risk sources.

Zumigo solutions help businesses across different industries verify and authenticate their consumers throughout the entire digital engagement journey.

Zumigo Addresses Key Use Cases Across the Entire Journey

Zumigo addresses the following key use cases to prevent revenue and consumer loss from fraud; improve user experience; accelerate business growth; reduce operational expenses; and comply with fraud and risk management requirements.

Use Case: Securely Onboard a New Consumer

Fraud occurs when a bad actor originates a new account using all or parts of someone else's personally identifiable information (PII) – including information from credit cards, banks, insurance, utilities, healthcare, brokerages, or e-commerce accounts. Because of data breaches, hacking and other scams, most PIIs have been leaked and are easily accessible by career criminals. Many types of fraud can pass traditional identity verification checks, including Know Your Customer (KYC). Zumigo helps businesses safely open new accounts for the legitimate consumers by:

- Comparing the name and address provided by the consumer to the name and address on file with the mobile carrier
- Returning mobile account information and risk indicators including account standing, account status and tenure, and any information on deactivation, SIM changes, porting, etc.
- Providing risk scores to indicate whether the phone is trustworthy and protected from account takeover; and whether the associated email belongs to the consumer
- Verifying other variables, including Anti-Money Laundering (AML) compliance, bank account, age limits, etc.

Zumigo

Use Case: Improve Conversion Rate with Secure Pre-fill Forms

Filling out personal information on a mobile phone with small virtual keys is a high friction, high frustration experience for consumers. To speed up the account origination or checkout process, auto form fill and express mobile checkout automatically populate mobile forms with the verified personal information, thus increasing the rate of conversion, speed of checkout, and consumer satisfaction.

Zumigo passively verifies the mobile number from the device, and upon verification, auto-populates additional information from the carrier such as the name and address on file. In the case of express mobile checkout, the credit card information can also be retrieved based on consumer's choice of payment method.

Use Case: Account Takeover Prevention

ATOs happen when fraudsters use stolen credentials to gain unauthorized access to consumer accounts where they can harvest PII; steal credit card information, cash, and loyalty points; purchase goods and ship to a different address; and access subscriptions at no cost, like streaming services. Such unauthorized access can result in negative impacts to the businesses.

Zumigo authenticates a consumer's mobile identity using authoritative data such as the mobile phone number, account activities, and other PII and behavioral information on file. Using real-time, definitive sources and through a layered approach, Zumigo can instantly detect fraudulent use of an identity for unauthorized account access and purchases across digital channels.

Use Case: KYC Compliance

Financial institutions and other regulated entities must follow compliance requirements to verify the identity of their consumers as part of KYC, AML and Counter-Terrorist Financing (CTF) efforts worldwide. The components include verifying the basic identifying information of every new consumer; understanding the consumer risk profile; and continuously monitoring consumer accounts and transactions for suspicious activities.

Zumigo provides the verification and authentication solutions to verify consumer profile via:

- Matching PII such as name and address, mobile phone number, driver's license, etc.
- Screening against required local, regional and governmental information sources including the Specially Designated Nationals and Blocked Persons (SDN) list, maintained by the Office of Foreign Assets Control under the U.S. Department of the Treasury; Politically Exposed Persons (PEPs) lists, maintained at a regional- and country-level; adverse media or negative news available publicly; and civil and criminal public records

Use Case: Protect Online Transactions

Online purchases made with stolen payment card information cost merchants millions of dollars in chargeback expenses, operational resources and time needed to resolve disputes, and lost revenue from unretrievable products. Such card-not-present transactions are risky and easy for bad actors to take advantage of. Zumigo helps businesses reduce chargeback risk by ensuring that the credit card and mobile phone belongs to the shopper making the purchase. Zumigo performs the following checks to provide trust scores on transactions to help merchants decide whether to complete fulfillment:

- Whether the name and address provided by the shopper match what's on file with the mobile network operator, or the credit card to validate the payment method
- If the mobile phone is in a location that makes sense for the transaction
- The distance between the mobile phone's network location and the following locations: merchant address, IP address, device (Wi-Fi SSID), or any other submitted set of geo-coordinates
- The geo-coordinates and address of the mobile phone's network location for the business to calculate the distance between the location of the phone and other pre-determined locations

Use Case: Unify Signals to Monitor Risks of Fraud

Bad actors source PII that includes a mobile phone number along with a list of passwords and websites where the passwords are registered. With this highly personal information, they script attacks to hack into as many banking, e-commerce and other types of accounts of the consumer as possible. Often, businesses do not have real-time visibility into these fraudulent attempts and are not able to take appropriate preventive measures in a timely manner. They unintentionally allow bad actors access to consumer accounts, resulting in financial harm for the consumer and reputational harm to the business.

Zumigo leverages the intelligence gathered from mobile phone activities across a network of businesses, including banks, FinTechs, neobanks, insurers, online merchants and retailers, to determine the risk of fraud. With trust scores based on analyzing a variety of real-time factors, businesses can pre-emptively prevent ATOs and PII harvesting.

The Consumer Digital Engagement Journey

Use Case: Reduce Friction, Streamline Consumer Experience

User names and passwords are still the most popular method of security and authentication of a consumer's digital account today. But it's unsecure, cumbersome, and expensive to maintain. Passwords create friction, frustration, and degrade experience as passwords can be lost, forgotten or impacted by breaches. Zumigo improves consumer sign-up/sign-in experience with secure passwordless access to reduce friction, improve security, and enhance experience.

Using mobile network authentication, Zumigo instantly verifies consumer identities using their mobile phone number or the installed passkey, with additional, layered protection using SMS/voice, email, or QR code one-time passcode (OTP). Legitimate consumers are allowed to access their accounts without entering passwords, whereas fraudsters are prevented from hacking the network.

Additionally, Zumigo reduces friction by automatically and securely filling shipping and billing information during the checkout process.

Use Case: Enhance Authentication Security

When a password reset request is issued, or when businesses need multi-factor authentication to keep accounts safe from hacks and breaches, an additional authentication method such as phone ownership and possession verification, or device enrollment verification, can be utilized.

Zumigo can issue OTPs by SMS link or voice to landline, email or QR code to verify that the mobile phone number belongs to the consumer and that the device is in the hands of the same person. Upon entering the passcode, Zumigo compares the existing consumer's name and address to the name and address on file with the carrier and returns a set of risk signals and scores. With SMS link, Zumigo can passively authenticate the mobile number in session. Additional verification step can be performed using mobile network authentication before the OTP is sent.

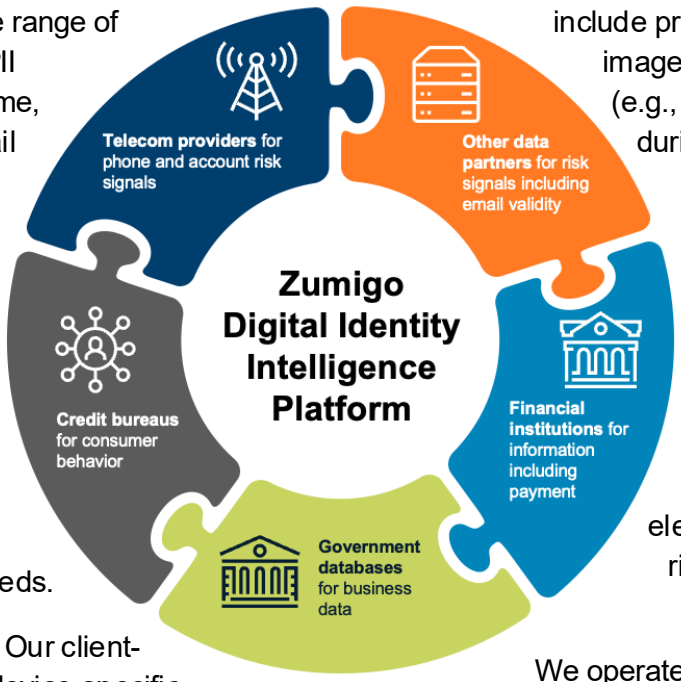
Alternatively, Zumigo can also authenticate the consumer's identity using passkey technology installed within an enrolled device that has been paired with the their account.

The Zumigo Digital Identity Intelligence Network

Zumigo builds a set of identity fraud prevention products and solutions upon a robust, real-time platform that offers a unique set of services and capabilities. At the core is the proprietary Digital Identity Intelligence Network. This network forms the foundation of trust by leveraging diverse, real-time, and authoritative data that offers a comprehensive view of the consumer identity:

- **Direct Carrier Integration:** Deep integrations with over 800 global MNOs provide unparalleled access to real-time subscriber information and network-level signals. This includes critical data for mobile network authentication, SIM swap detection, call forwarding status, number porting, and device deactivation alerts – offering accuracy of the verification not available through indirect means.

- **Extensive Partner Identity Network:** We integrate with a wide range of vetted partners for PII verification (e.g., name, address, DOB), email intelligence, bank/ payment account validation, and broader risk assessment. The partners are part of a proprietary orchestration network, and configured to meet specific business needs.
- **Device-Level Data:** Our client-side SDKs capture device-specific information, including device fingerprinting and behavioral biometrics, for a richer assessment of risk.



- **Consumer-Provided Data:** Our capabilities include processing identity document images and biometric information (e.g., selfies for liveness checks) during the verification process, to enable step-up authentication in account onboarding or in high-risk transactions.
- **Data Analysis and Risk Scoring:** We employ robust analytics to process these signals, connect PII elements, and provide holistic risk scores and granular risk indicators.

We operate with a strong emphasis on privacy and security by design, adhering to global regulations and protecting PII. We are ISO 27001 and SOC2 Type 2 certified.

Zumigo Solutions For Flexible Deployment

Via API: The Zumigo platform can be integrated via API to existing architecture to access an ecosystem of digital identity information instead of integrating with each provider. The Identity Service API lets businesses select and customize the verification workflows, featuring the following:

- The connection is secured with HTTPS and multiple authentication methods
- Requests are sent via JSON, with fast real-time responses received
- One single API supports multiple requested data elements
- Access to a scalable platform with high TPS support

Via low-code/no-code platform: The platform provides a visual interface where a user can easily create the onboarding and authentication workflows from a menu of available services. The workflows can be embedded in the customer's website/app or be hosted by Zumigo. A dashboard provides a view into key verification metrics, event log, device finger-printing intelligence, support, and billing, etc.

Via marketplace: Some of Zumigo's solutions can be accessed as plug-and-play apps on major e-commerce platforms.

- Zumigo OrderRisk is available on Shopify and BigCommerce.
- Zumigo InstaAuth is available on Shopify.

The Zumigo Suite of Products

Zumigo Assure Identity leverages real-time data from authoritative sources, including mobile operators, credit bureaus, financial institutions, and other data partners, to offer a match/no match verification of digital identity belonging to an individual or business.

For an individual, Zumigo verifies the following:

- Associated PII including name and address, phone number ownership, and other mobile phone subscriber information
- Returns match scores and confirms mobile phone ownership, helping meet KYC requirements and prevent identity theft
- Payment identity for bank account status and credit card accounts
- Email validity covering a variety of email-related verification, including ownership and other PII associations

For a business, Zumigo verifies the following:

- Associated business information such as address, phone number, incorporation date and type, industry classification number, etc.
- Person of contact and principal identity
- Ultimate Beneficial Owner (UBO), list of executives, officers and employees; and whether there are any on the SDN list, maintained by the U.S. Department of the Treasury
- Financial data including sales and revenue

Why Zumigo Assure Identity?

- Satisfy KYC, Know Your Business (KYB) and age restriction compliance requirements when consumers volunteer their phone number for authentication
- Prevent linkage of valid bank account to fraudster's digital payment account where funds can be stolen for fraudulent purchases
- Establish trust at sign-up/sign-in and offer consumers a frictionless experience
- Prevent revenue loss due to fraud/risk from identity theft and PII manipulation, and returned or rejected payments
- Protect customer trust and build brand reputation

Zumigo Assure Authentication enables seamless, secure first-time sign-ups and returning passwordless sign-ins for consumers. It prevents identity fraud and account takeover while eliminating mobile, computer and tablet authentication friction. The product comprises the following technologies:

- **Mobile Network Authentication:** Zumigo captures the phone number passively from a mobile device's cellular signal with the MNOs to verify possession and ownership. It works by using a process called header enrichment to automatically identify the MNO assigned phone number for the device, or by authenticating the Subscriber Identity Module (SIM) in the mobile device via carrier networks and application providers.
- **One-time passcode:** Zumigo generates and sends OTPs to the consumer's mobile phone via SMS, SMS link, voice OTP, email, and QR code, and verifies the passcode when it is entered into the app or website. Before sending the passcode, Zumigo can first assess the account takeover risk of the

consumer's mobile phone. This step ensures that the passcode is received by the intended device instead of a scammer's, to prevent fraud.

- **Passkeys:** an asymmetric key pair is generated after verifying mobile phone number possession and ownership during enrollment. The private key is stored in the secure enclave of the mobile phone and the public key, now associated with the verified mobile number, is shared with the server. Subsequent logins via the same device will bypass the sign-in process, resulting in a frictionless experience.

Any of these methods can be layered with other verification and authentication methods for more protection and risk insights to determine trustworthiness, especially for high-value transactions or accounts. Additionally, these technologies also allow the transfers of the authenticated and verified trust from the mobile phone to a desktop/laptop/tablet so that the consumer can sign into an online application without using user names and passwords.

Why Zumigo Assure Authentication?

- Verify the owner is in possession of the phone without unnecessary friction
- Improve consumer experience during account opening or sign-ins by using seamless, low friction authentication methods
- Satisfy KYC requirements when consumers volunteer their phone number for authentication and verification

Zumigo Assure Insights brings together real-time information associated with the consumer's digital identity for a holistic score that represents the trustworthiness associated with the account holder and the transactions initiated by the consumer. This helps businesses make smart decisions on whether to trust the digital identity and transaction, and allow access to digital accounts. Push or batch alerts can be delivered at pre-configured time intervals for monitored phone numbers to proactively prevent identity fraud. The trust score assessments Zumigo offers include:

- Risk signals associated with the mobile phone, including SIM swaps, porting, call forwarding, deactivation, etc.
- IP-based location intelligence for detecting anomalous access patterns and high-risk geographies
- Email trust score base on real-time information such as domain name risk (reputation and authenticity, country, type) and email details (tenure, first and last date encountered/identified, frequency, social media association, last time fraud was reported, etc.)
- Risk of account takeover fraud based on the different risk signals listed above
- Trust of a mobile phone number by analyzing a variety of related real-time and suspicious activities (e.g. deactivations and porting events) across a network of businesses
- Detect mobile phone number risk based on status changes for registered phone numbers, and sends updates and alerts at pre-configured time internals so that businesses can pre-empt a potential fraud attack

Why Zumigo Assure Insights?

- Proactively stop fraud by assessing

consumer and transactional risks based on the consumer's mobile identity and behavior, using a comprehensive portfolio of signals

- Detect account takeover (SIM swap, porting, call forwarding) risks to protect consumers, accounts, brand reputation and the business' bottom line

Zumigo DeRiskify provides a comprehensive security and fraud prevention suite for e-commerce merchants. The suite of products leverages deterministic digital consumer information from authoritative sources to authenticate shoppers at the point of accessing e-commerce services with low friction, and verify payment methods to stop fraud before orders are processed. This helps businesses maximize conversions while reducing fraud losses by eliminating chargebacks.

For shopper authentication:

- Merchants can offer passwordless log-in/registration and onboarding option to reduce shopper friction and increase conversion
- Instantly verify shoppers on their phone with additional, layered protection using email or SMS OTP
- Merchants can utilize the dashboard for insights to shopper log-in information: method of log-in (mobile network authentication, SMS OTP, email OTP), device OS, IP address, IP location, network type, browser, timestamp, device, shopper name, phone number, mobile network operator, line type, IP and other phone details
- This product is packaged as Zumigo DeRiskify InstaAuth app on Shopify and BigCommerce, or can be custom-integrated

For order risk verification:

- Verify orders using SMS verification for textable numbers and voice call for non-textable numbers to confirm phone possession
- Validate the name and address associated with the phone number and payment instrument; IP address of the shopper's browser client; email address validity; and geodesic distances between billing address, shipping address and customer IP address
- Provide trust scores based on the above for each transaction so that a merchant can choose to fulfill only the low-risk transactions
- Provide a dashboard view of the transactions so that merchants can see how their purchase orders are performing at a glance or drill into each transaction for more information: number of total transactions, high risk orders, high risk customers, fraud orders processed and related value; type of merchandise that is high risk; and location/origins of risky transactions
- This product is packaged as Zumigo DeRiskify OrderRisk app on Shopify and BigCommerce, or can be custom-integrated

Why Zumigo DeRiskify?

- Reduce authentication friction in shopper experience
- Improve conversion rates by eliminating passwords

- Protects e-commerce merchants from fraud losses by preventing disputes, chargebacks, and revenue loss due to identity theft
- Verify the shopper with authoritative sources to comply with KYC requirements
- Grow shopper trust, reduce negative sentiment as a result of fraud

Summary

By leveraging real-time, authoritative MNO, device and other third-party data, Zumigo eliminates the critical security risks and high operational friction associated with traditional single-focused identity fraud risks prevention solution. The multi-layered verification and authentication framework proactively stops fraud before the resulting security risks and loss occur. Zumigo empowers enterprises to reduce the identity-related vulnerabilities in the digital perimeter; maximize conversion rates; and build lasting customer trust through intelligent, seamless security.

Zumigo solution is:

- **Real-time:** Zumigo authenticates consumer identity using real-time information sources. The resulting risk signals instantly adjust and respond to suspicious events, so that fraudulent activities are prevented before they have a chance to materialize.
- **Authoritative:** No static history or outdated predictive analytics! Zumigo uses authoritative information from multiple sources to provide conclusive risk scores. Businesses can determine whether to approve or fulfill an activity or transaction.
- **Accurate:** With a multi-layered approach using real-time and definitive information sources, Zumigo reduces more false positives and negatives than other traditional verification and authentication methods. Businesses build trust with their consumers faster with Zumigo.

About Zumigo

Zumigo powers digital identity verification in the world's largest enterprises to protect transactions, accounts and trust, using real-time intelligence across mobile, email, device, financial, account, and other information sources. Its modernized, multi-layer approach fortifies the identity perimeter against today's complex fraud and promises a streamlined consumer journey from onboarding to transactions. Learn more at www.zumigo.com.