pipl

Online Identity and the Digital Economy of tomorrow

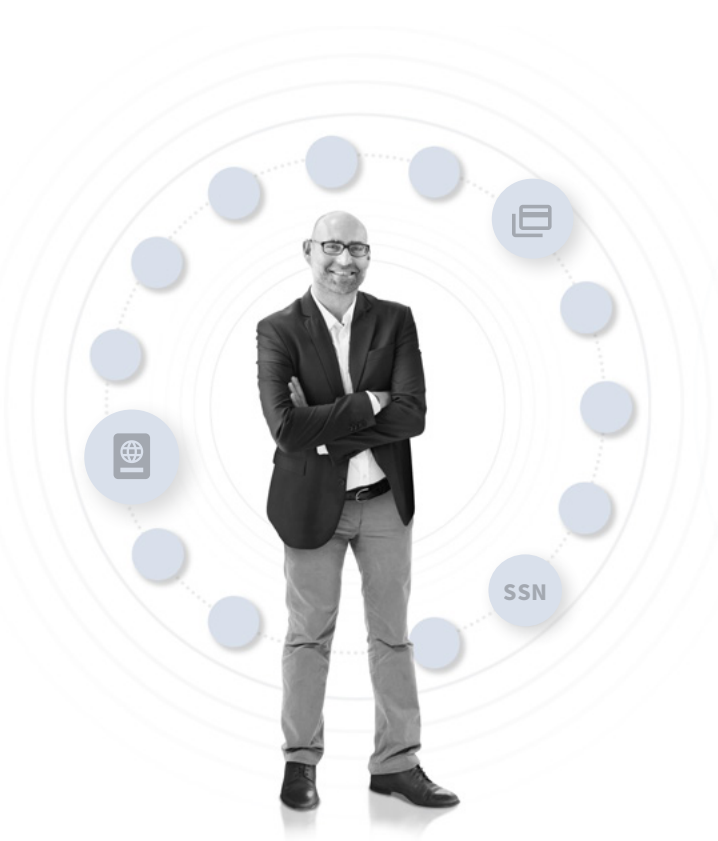
The Backstory

The digital payment and verification environment of today was established on an infrastructure designed for traditional credit and debit-based payment verification. Transactions relied on a card-present environment for safety and security. Identity was verified by the presence of traditional government-issued documents, such as a driver's license, social security number, or other state-issued identification. These provided unique physical links to the customer in the form of street addresses and phone numbers.

Additional verification elements were eventually added. Passwords and personal identification numbers (PINs) improved the security of traditional transactions, but they also increased customer friction and introduced a new generation of technology-related challenges.

As the 20th century became the 21st, organizations began migrating to online transactional environments and found it inadequate to continue to rely solely on their traditional verification infrastructure for transactional risk management. The balance continues to shift from traditional to electronic payment and online interaction, and organizations have had to develop fluid strategies to match the rapidly evolving threat and defense battleground of today's e-commerce environment.

As commerce has entered the digital age, the inadequacies of traditional verification and authentication methods have been exposed and amplified. The online world allows us to interact with countless strangers around the real world without any physical confirmation that they are who they claim to be. This demands that we develop new methods of assurance for the protection of our customers, our reputations, and our bottom lines.



The Current Environment

False positives, false negatives, and real challenges

Reliance on traditional verification methods alone falls short of meeting the needs of most digital organizations. It's becoming increasingly important, and often more difficult, to identify malicious users attempting to take advantage of an online environment. It's also becoming more difficult to identify legitimate users who may be demonstrating higher risk behavior than normal. Customers no longer conform to simple "high risk" or "low risk" patterns, giving rise to an increase in false-positive flags.

Unfortunately, the due-diligence required to confidently identify bogus transactions can have a negative impact on the experience of legitimate customers and bottom-line revenue.

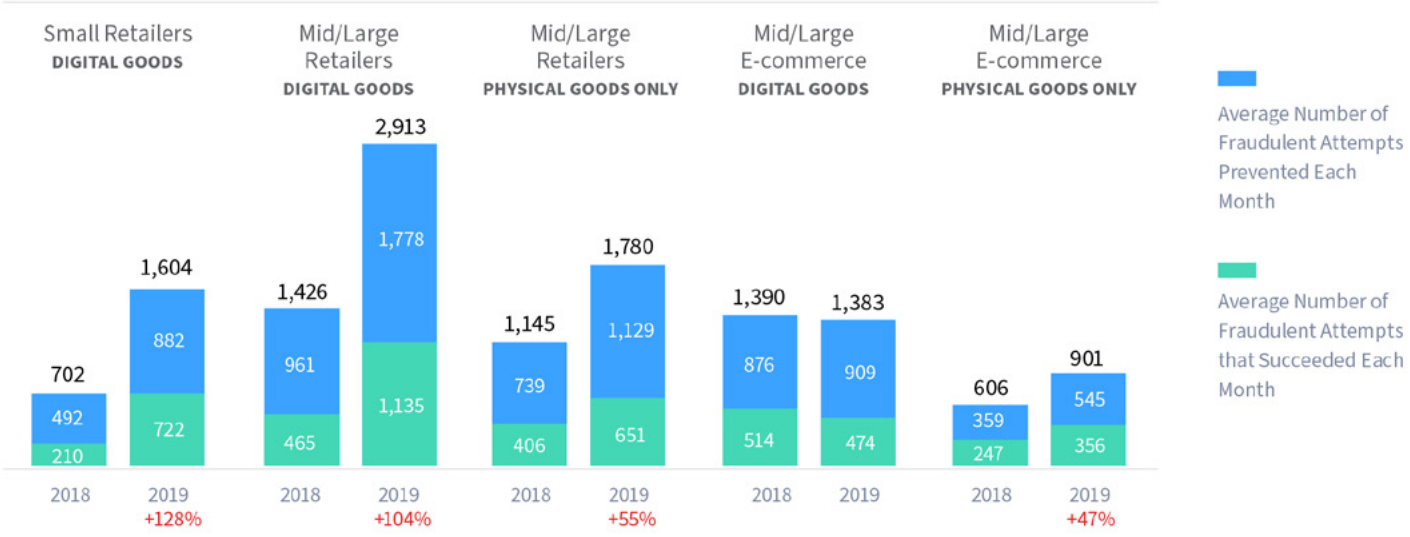
While identity verification is important, it's equally important to consider the legitimate customers who expect a frictionless experience and protection from misuse of their accounts and personal information. Transaction and account access activities such as account origination, user login, and account management must be familiar and safe, regardless of their contexts.

New threats

The battle against fraud is a fight against a constantly moving target—with the target moving faster and more erratically each year. Rapidly-evolving fraud risks and an increasingly digital economy are driving organizations to devote more resources to the development of defensive strategies in an effort to get ahead of the threat, but all too often, they're not even keeping up.

According to the 2019 LexisNexis "True Cost Of Fraud" survey, fraudulent transaction attempts are rising sharply.

Average Number of Total Fraud Attempts Per Month



The steep rise is being fueled by a dramatic increase in high-profile data breaches, leading to an increase in **Account Take Over** (ATO) attempts, which further erodes the effectiveness of traditional identity verification elements. Stolen identity files are now readily available on the deep and dark web, leaving the companies that rely on these compromised elements increasingly vulnerable to ATO-related breaches and malicious use of their customers' accounts.

Using a combination of real information that has been stolen and fabricated information, bad actors have been able to more easily create fraudulent accounts using synthetic IDs that they develop and nurture over long periods of time. **Synthetic IDs** are particularly difficult to detect with traditional means and even more difficult to predict, as the actual crimes can take years to manifest.

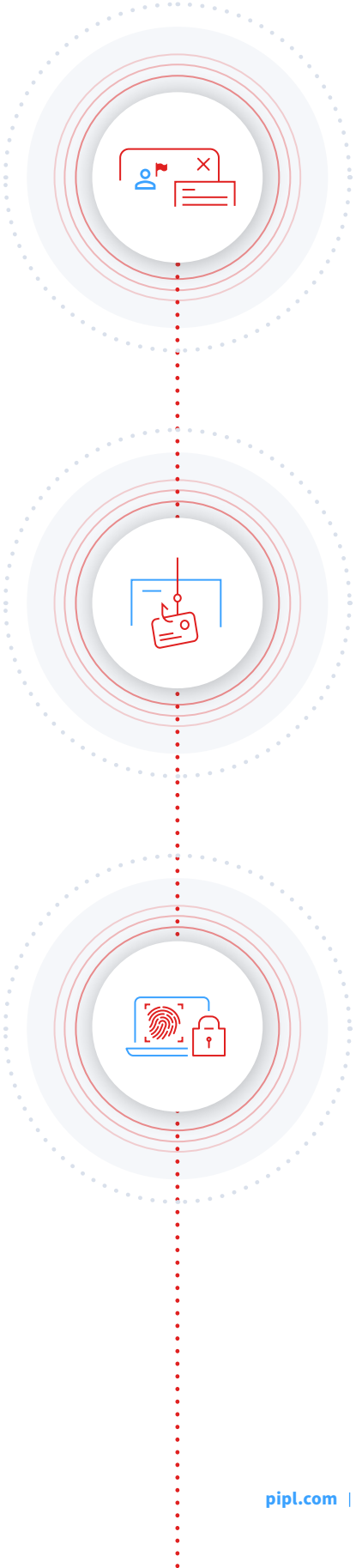
New account fraud is increasing as a result. With easy access to both offline data and payment credentials that satisfy the requirements of **card not present** (CNP) payments, it's become trivial to fake an online identity and establish an account that can be used for fraudulent purchases, funds transfers, and money laundering.

We've also seen an increase in **phishing attacks**. Like the large-scale data breaches, successful phishing attempts are funneling data into the hands of bad actors. While data breaches involve large groups of people, phishing attacks are more focused on vulnerable individuals. This is especially true in the case of "spear phishing" or "whaling," where users with high-level access to sensitive or valuable material are targeted as a means to access even more valuable and potentially damaging information.

Then there are regulations—confusing, conflicting, and inconsistently enforced laws such as GDPR and CCPA are making it more difficult to collect and retain information that can be used to detect and deter repeat offenders. Privacy and identity information regulation will continue to evolve and expand, and as it does, the sophistication of fraud prevention practices will have to keep pace.

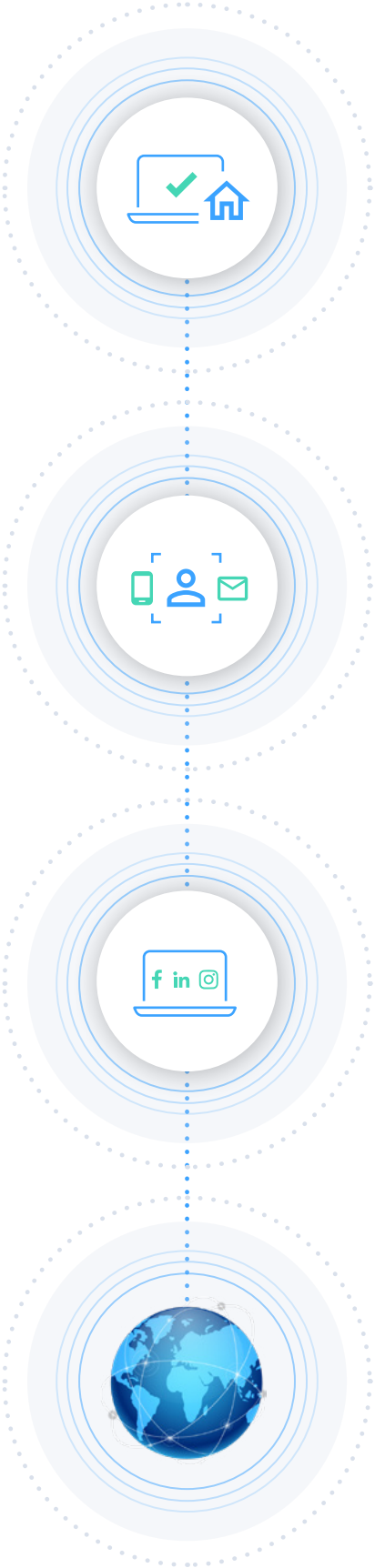
At the time of this writing, COVID-19 is still raging across the world and exacting a terrible toll. The related chaos has opened a door for the most unscrupulous to launch a wave of attacks on the desperate with credential phishing, malicious attachments and links, **business email compromise** (BEC), fake landing pages, downloaders, spam, malware, and ransomware. Fear and false hope are the lures for potential victims that lead to a range of dangerous scams. In recent weeks, malicious campaigns have emerged involving healthcare, pharmaceutical, and relief organizations offering bogus cures and fictitious aid channels that are defrauding the innocent out of money and hope.

These threats aren't entirely new but they are increasing at a rate that outpaces the growth of online transactions in general—a grim indicator that we are currently losing the battle against fraud.



Online & Offline Identity Elements: **More Powerful Together**

Battles aren't fought with a single defense strategy, and neither should companies rely on a single form of identity verification to detect and prevent fraud. The combination and corroboration of offline and online data enables a much more effective defense against modern threat tactics than traditional single-source methods.



Address verification

Address verification services (AVS) are a good first step to verify a connection between a credit card holder and a shipping address, but what can be done when there is a mismatch? It's not uncommon for customers to purchase goods on behalf of a family member, business, or associate located at an address other than the one connected to the card. While a simple check of traditional offline data can uncover the mismatch, it's not able to reveal potential relationships between the cardholder and the mismatched shipping address. For this, an online identity profile can reveal connections to multiple addresses of family members, businesses, and associates. Performing a reverse lookup of a street address with an online identity tool can also reveal insights about the person who is associated with the mismatched shipping address—for example, a person with the same last name, a business associated with the cardholder, or a person known to have a history of fraudulent behavior.

Email and mobile phone

Connections between names, mobile phone numbers, and email addresses are also reliable indicators of legitimate versus fraudulent intent. When these identity elements can be verified through a cross-referenced source or through multiple sources, the probability of legitimate intent goes up exponentially. The same is true in reverse: when elements cannot be verified through connection, they are more suspect.

Social and media sites

Usernames on social and media sites have evolved on a path in opposition to any attempt at linking them to real people. In fact, a visual inspection of a username often only hints at a relationship to a known person, or they can be entirely unrelated in meaning. However, linking multiple sources of data together can reveal connections to other known information that can link obscure usernames to robust online identities and vice-versa. This allows fraud investigators to establish connections to sources of information that would be difficult and time-consuming to achieve by other means.

Global data

In a global economy where transactions across country borders are common and essential to the existence of many businesses, a source of identity data with global coverage is required. Many single-source data providers offer only US or locally-based identity information. Businesses that rely on growth in foreign markets know that risk increases disproportionately as transactions reach across borders, but so does the opportunity to gain share in new markets. These companies are discovering that risk can be greatly reduced if a connection to an online identity can be established.

As organizations seek better methods of fraud control and customer protection, they have become aware of a need to develop solutions that are unique to their business and environment. They've discovered that a one-size-fits-all approach to identity verification isn't enough to gain an upper hand against fraud and unwarranted chargebacks. Many organizations are creating effective toolkits by integrating multiple tools and data sources into their processes. Some are incorporating their own machine learning and artificial intelligence technology to optimize decision-making for their unique customer base and product offerings.

Automation

Automation is necessary when processing large volumes of transactions. It's most effective as a first check in the process. The automated connection of information supplied by a customer to verified offline and online sources improves decision confidence and can automatically segregate the riskiest from the least risky transactions.

An automated solution might derive a score based on the number of matched or connected identity elements. It might go on to automatically adjust the weight of those scores as it identifies patterns with certain elements. For example, it may determine that customer email addresses that have connected social media accounts with a data history of more than two years are extremely unlikely to be fraudulent, or that the absence of connected social media accounts when a shipping address mismatch is detected indicates a high likelihood of fraud.

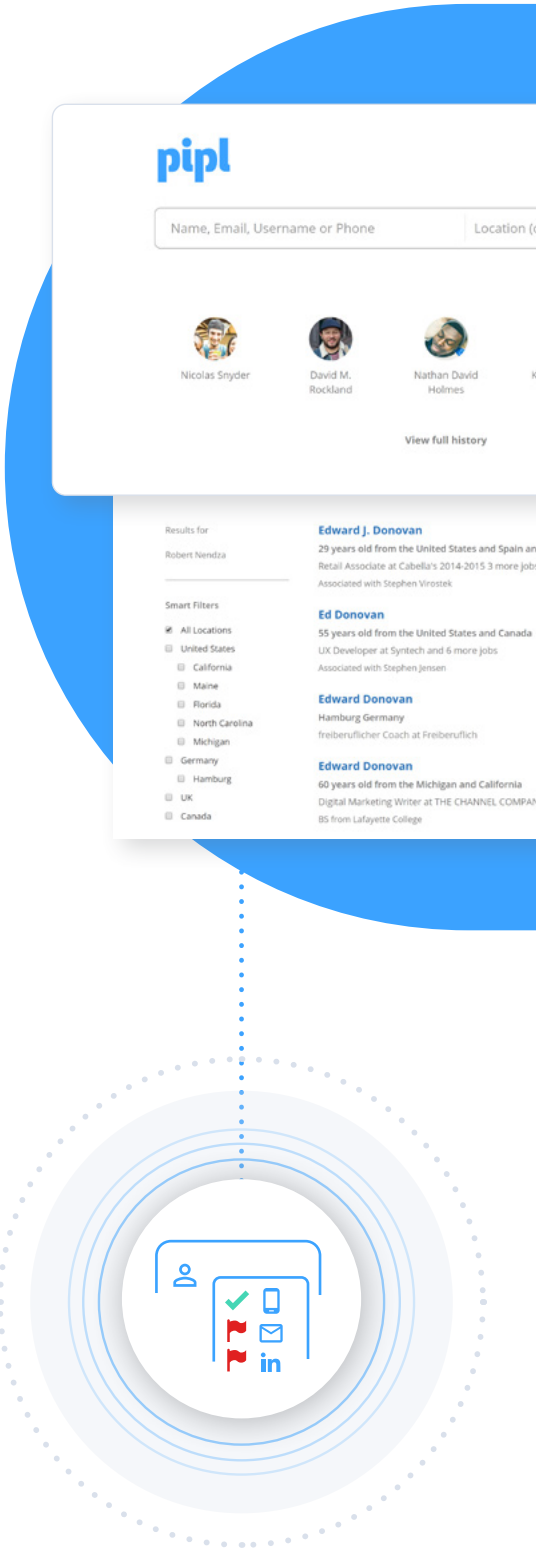
Whether or not the algorithms are adjusted manually or by virtue of machine learning, automation gives the advantage of data-driven decision making to the companies that have the capability.

Manual Review

Manual review is commonly the second step in a fraud detection process. When anomalous activity or data is detected, a system typically responds by either rejecting a transaction or passing it to another system for additional review. That review is often performed manually.

Fraud analysts with access to online identity information approve transactions by verifying multiple points of personal information including the customer's age, email addresses, mobile phone numbers, and social usernames. Speed is of the essence in manual review, both for the sake of the customer experience and for the efficiency of the manual review operation.

Not long ago, credit card customers had to either notify their card issuer prior to an unusual trip or risk having their accounts suspended for suspected fraud. This friction point is now largely avoided due to the connection of credit cards to email addresses, email addresses to mobile phone numbers, and mobile phones to social media accounts. Now fraud analysts have tools to quickly determine if overseas or out-of-area charges are due to travel or stolen identity information.



ATO-based fraud can be detected by the presence of questionable changes to existing account information that can be connected to entirely different online identities. By identifying inconsistencies between new and existing elements, analysts are able to quickly and confidently identify ATO fraud.

Both

The most effective anti-fraud systems utilize a combination of tools and methods. Generally, the more that can be automated the better, leaving only the most nuanced high-value decisions for manual review. The adaptability of the systems to behavioral changes, environment, and the ever-evolving threat landscape is also crucial to the success and maintainability of the system.

It's difficult to say if, or when, there may be commercially-available systems that automatically configure themselves and adapt to unique environments. For now, it appears that the most effective fraud defense and protection system is a custom tech stack that connects user-supplied data to an online identity, and a two-step process of automation and manual review.

For now, it appears that the most effective fraud defense and protection system is a custom tech stack that connects user-supplied data to an online identity, and a two-step process of automation and manual review.

Benefits of an integrated multi-step fraud system:

- Higher decision confidence
- Frictionless customer experience
- Customer account and data protection
- Higher transaction approval rate
- Higher fraud detection/prevention rates
- Regulatory compliance
- Greater market reach
- Operational efficiency

Pipl Online Identity Information

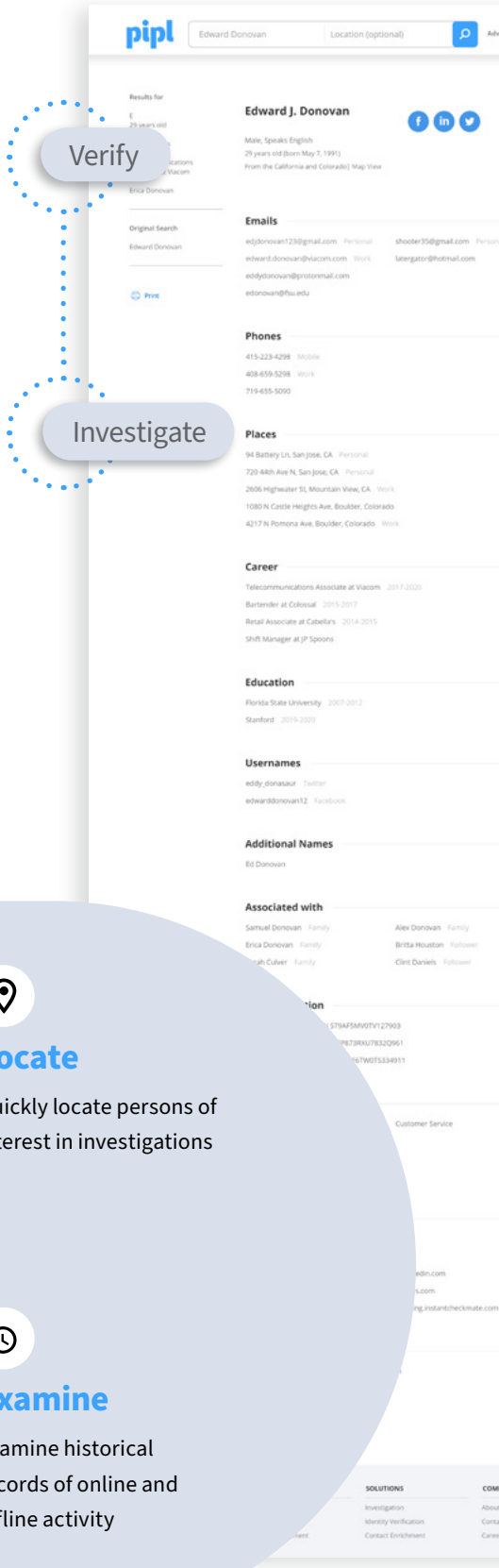
Pipl is the leading provider of online identity information. With unmatched global coverage of over 3 billion online identities that have been cross-referenced and assembled from over 25 billion individual identity records, Pipl gives professionals information and tools to confidently identify fraud and protect legitimate customers.

The overarching value of the Pipl online identity solution is the ability to identify and validate a person, and to determine their trustworthiness and intent.

Pipl SEARCH is an intuitive SaaS search application that offers detailed personal, professional, social, demographic, contact, and relationship information in the form of an interactive profile. The solution is ideal for manual review, investigation, research, and analysis.

Pipl SEARCH allows professionals to perform searches on a wide variety and combination of inputs that instantly generate a robust identity profile containing names, birth dates, email addresses, physical addresses, landlines, mobile phone numbers, cars, associated people and business, social media account links and known usernames. Each data element also contains meta-information including data types, sources, and historical first/last seen dates.

A quick scan of a Pipl profile can verify the information a customer enters during a transaction or new account setup while the detailed information can speed an investigation by uncovering critical details that lead to stronger cases and better resolution rates.



Manual review using online identity information:

Verify

Verify customer input

Detect

Detect and approve unusual behavior by legitimate customers

Investigate

Investigate patterns common to the use of synthetic IDs, stolen information, and the probability of fraud and malicious intent

Locate

Quickly locate persons of interest in investigations

Connect

Connect to personal, professional, and social information

Uncover

Uncover associations between people, addresses, phones, and social handles

Determine

Determine the credibility of sources, witnesses, or suspects

Examine

Examine historical records of online and offline activity

Pipl API helps companies automatically verify identities across their decision platforms. Pipl API powers risk assessment for a wide range of the world's top e-commerce, financial, and compliance-sensitive businesses. Pipl's API customers have access to a comprehensive data API with developer-friendly client libraries and code samples for popular languages to easily add real-time identity information to their applications.

Pipl API puts the power of over 3 billion online identities to work in your application. This is ideal for automated identity verification, fraud, and investigation support.

Through these two approaches, Pipl helps users take what they already know and validate it against identity information collected and corroborated from many sources. This can be achieved using traditional offline details mentioned above, such as associated contacts, physical addresses, relatives' locations, plus digital persona-driven behavior online, which is increasingly harder to fake.

This combination is powered by Pipl's High-Performance **Identity Resolution Engine**, which includes the following elements:

Pipl Identity Index

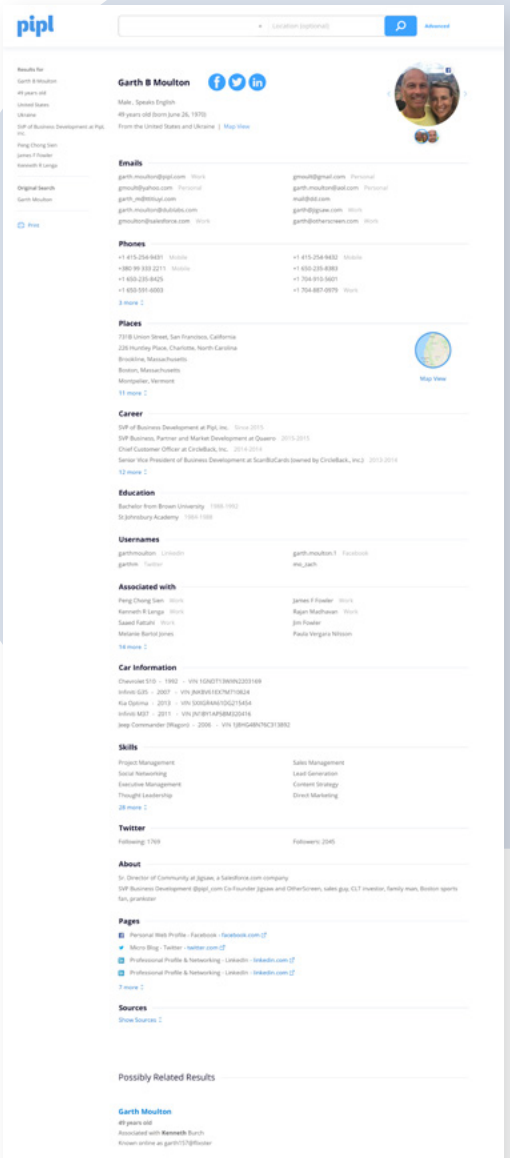
Pipl's ethically and legally sourced data is a collection of many billions of data points compiled from the internet, public records, listings, directories, archives, and exclusive sources.

Pipl Identity Algorithms

Proprietary clustering algorithms identify and cross-reference related data among countless possibilities to build highly accurate identity profiles in real-time.

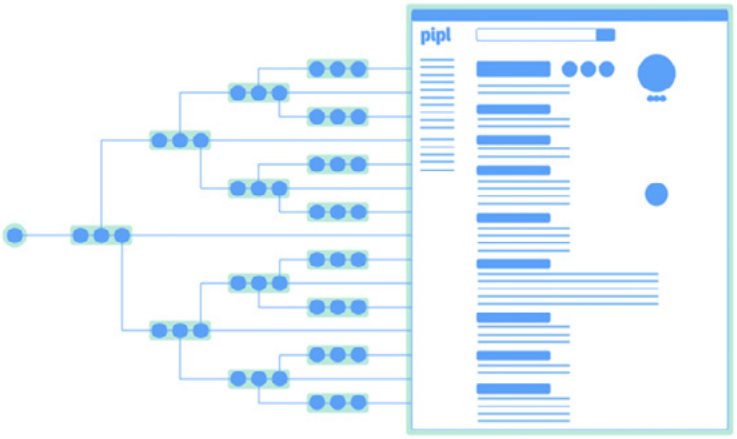
Pipl Identity Profile

A Pipl Identity Profile includes email addresses, mobile phones, landlines, social media accounts, online accounts, usernames, address histories, career and education histories, motor vehicles, associations (work, family, online followers), photos, videos, and more.



Recursive Search Algorithm

There is a lot of information out "there." Finding information from a single source on the internet is simple but even less trustworthy than relying on a single traditional identity source. The real value of an online identity comes from the collection and corroboration of data from many sources. This is where Pipl excels. Their recursive search algorithm follows a multi-step search process:



Pipl's recursive search algorithm parses the individual elements of each matched record and recursively runs additional searches using the found data as a new input.

Pipl's recursive search algorithm finds multiple matches to input just like a common search engine—but it doesn't stop there. It parses the individual elements of each matched record and recursively runs additional searches using the found data as a new input. This uncovers more matches but more importantly, it corroborates data across many sources, vastly increasing the depth and reliability of the information.

For example, a user may input an email address, mobile phone number, or street address. The engine may find several identity records that match the input. Several of those records may include a name. Others may contain references to other people, businesses, or social media profiles. The algorithm takes each element and runs additional searches looking for matches to data that was not originally searched for. This has the effect of running dozens of searches against countless online and proprietary data sources, then compiling the results into a single high-corroborated identity profile.

This result would be virtually impossible to achieve without the existence of a massive identity index and a sophisticated clustering algorithm to identify and make sense of the often obscure connections between various sources of identity information.

Corroboration is King

Faking or lying about a little bit of information is relatively easy. No system or algorithm is foolproof, but a highly-corroborated online identity makes it extremely difficult, or at least not worth the trouble, for a person with ill-intent to fabricate.

Government documents and offline data elements can be helpful, but verification can be difficult and prone to increased customer friction and technological complexity. By moving beyond traditional validation methods and leveraging digital elements in the form of an online identity, organizations can grow more confidently and safely in the online world.

Pipl online identity information allows reviewers and investigators to essentially search with "anything" (name, email, phone, age, address, associations, education, jobs, etc.) to find "everything."

Preparing for Tomorrow

The risk of fraud goes well beyond a simple cost of doing business. In today's era of crowdsourced reputations, businesses can't afford to alienate even a few customers. Reputations that have taken years or decades to develop can be shattered overnight. On the flip side that coin, news of a vulnerability, or a reputation as an easy target, can spread among the fraudster community faster than most businesses can react.

Organizations must develop and maintain an adaptable system for fraud detection and prevention.

Multi-stage defense strategy

Even low-volume operations require multi-stage fraud processes to compete in the battle for customer loyalty and fraud prevention. Effective systems begin with traditional checks and balances designed to flag anomalous and suspicious activity. This is typically the domain of the payment systems being used and is sometimes augmented with internally developed rules engines or, in more advanced systems, machine learning and artificial intelligence algorithms. The next stage involves verification of the known data. When a flag is raised, you must take what you know, usually a combination of information the customer has entered and information you get from a payment processor, and verify that it does indeed point to a real person. This is where online identity information can quickly draw connections from singular, easily-faked sources to a customer profile with numerous data points that have been corroborated by multiple independent sources.

Verification is often all that is necessary to make a confident judgment—but not always. By definition, anomalous activity means that something doesn't conform to expected patterns. Human investigators must be able to see and follow data connections that are difficult for simple algorithms to discern. Connections to identity history, family members, friends, businesses, and social media sites often lead to an explanation of the anomaly—giving decision-makers a much better basis on which to make confident judgments.

The final stage is to make a judgment based on what is known and what has been discovered. This can be automated to a point, but often requires manual intervention. The key to this step is the presence of reliable connected information. Automated decision-making is exponentially more accurate when the data is plentiful and reliable. The same is true for human decision-making, but even more critical then, is knowledge of the broader context of the person and the transaction.

Steps in a multi-stage fraud process:

Detection › **Verification** › **Investigation** › **Judgment**

Global markets

Organizations may have their own reasons to embrace, fear, or ignore global markets, but cross-border transactions are inevitable in virtually all online offerings. Traditional identity data providers don't often maintain or have access to consumer data in geographies outside of North America. Traditional consumer information is based on bank data which is lacking in areas with high numbers of unbanked or under-banked individuals. This is even more true of demographically younger markets where individuals have less credit history and consequently less traditional identity information.

As economies become more geographically fluid and more risky, a solution can again be found in online identity information. Online identities can greatly reduce risk when the input can be matched to a profile containing information from multiple corroborating sources. Many organizations turn to Pipl for their unmatched global coverage that includes mobile phone numbers and social media connections in addition to email addresses and home addresses.

Regulatory compliance

Government bodies and industry organizations have reacted to the rise of online fraud and a growing sensitivity to personal identity information (PII) privacy and security with an ever-expanding list of regulations. GDPR and CCPA have been mentioned previously, but regulations related to anti-money laundering (AML), know your customer (KYC), and age-appropriate content have put additional pressure on merchants and financial institutions to employ identity verification and investigation practices that meet the requirements.

Like the cost of fraud, the cost of regulatory non-compliance goes beyond the obvious. Violations and legal battles rarely go unnoticed by the public and can add insult to injury in the form of damaged reputations on top of the legal fees and potential fines.

It's important to consider how you will address responsibility for regulatory compliance. Some aspects of compliance will fall solely on the shoulders of your organization while others may be shared with third-party data providers. You must work closely with partners who are themselves compliant and transparent about their data collection practices and sources.

None too soon

The sea change to a digital economy may not be headline news anymore, but recent events have shown a bright light on the need for online identity data to augment traditional forms of identity verification. The COVID-19 pandemic, along with widespread political and social unrest, has only made the battle against fraud and the protection of personal identity information that much more urgent.

Organizations must address fraud head-on for the sake of their customers and businesses. Traditional methods are no longer sufficient by themselves, and online identity information can fill the gap.

Pipl is evolving to stay ahead of the needs of organizations engaged in online transactions. Their massive identity index is unmatched for its global coverage and proprietary algorithms connect traditional identity data to robust online identities for verification and investigation capabilities that keep pace with the evolution of the digital economy.

Organizations must address fraud head-on for the sake of their customers and businesses. Traditional methods are no longer sufficient by themselves, and online identity information can fill the gap.

ABOUT PIPL

Pipl is the world's leading provider of online identity information. With unmatched global coverage of over 3 billion online identities compiled and cross-referenced from over 25 billion identity records, Pipl is the choice of professionals worldwide.