WHITE PAPER

The Trust Paradigm for Online Business

Why trusted identities are essential to building a safe, trusted online world

pipl®

Trust: A Pivotal Issue for Everyone

Online engagement is shaping the world. It's driving digital transformation of businesses and governments. It's connecting people with common interests around the world. It's giving people a voice—and at the same time, being used to influence and manipulate opinions and events. As in every area of human endeavor, there are both good guys and bad guys. Online however, it's easier for bad guys to hide or look like good guys. And it's easy for bad guys to make good guys appear like villains.

Who can you trust? It's difficult for companies to quickly discern trustworthy organizations and individuals online—especially without the right tools. For this reason, digital trust and safety is emerging as a pivotal issue.

What if you could focus on looking for good interactions with trustworthy people instead of endlessly hunting for bad actors and their tactics? And what if it was easy to identify trusted customers, subscribers or users? The impact would be felt on everything from revenue to customer satisfaction and brand value.

What if you could focus on looking for good interactions with trustworthy people instead of endlessly hunting for bad actors and their tactics?

In this paper, you'll gain context about the global trust problem, how cyber criminals and fraudsters manipulate or abuse trust in the online world and learn why trusted identities are a key to establishing digital trust and safety across the internet and beyond.

Establishing Trust is a Global Challenge

Digital trust and safety is a global concern. According to DataReportal's Digital 2022: Global Overview Report, there are 5.31 billion unique mobile phone users, or 67.1% of the world population. Internet users total 4.95 billion, or 62.5% of the population, and there are 4.62 billion active social media users, or 58.4% of the population—and the typical user spends seven hours a day connected to the internet across devices. This means that a majority of people in the world are encountering brands and people online most of their waking hours.

This makes us targets. Authentic brands are making Herculean efforts online to deliver courteous, frictionless experiences to their customers and followers. Whether selling products, creating an experience or offering a public forum, positive engagement drives business and loyalty, extending customer lifetime value. Yet fakes, frauds and fools are just as committed to stealing money and data, posting misinformation and fake reviews, preying on vulnerable people and sabotaging reputations.

Fraud Prevention Isn't Enough

To date, efforts to identify and foil fraudsters' intentions have focused on preventing financial loss and brand damage. As cybercrime and fraud have steadily grown, organizations across all industries are increasingly adopting fraud detection and prevention solutions. According to Fortune Business Insights, the global fraud detection and prevention market size was $25.66 billion in 2021 and is expected to grow from $30.65 billion in 2022 to $129.17 billion in 2029.

Solely focusing on fraud prevention is obviously not enough. Organizations are still—and will always be—chasing fraudsters and trying to anticipate rapidly changing fraud patterns. What's more, there are many types of fraud that traditional fraud-prevention solutions aren't well equipped to handle. For example, profile misrepresentation—which grew 6.5% between 2019 and 2021, according to the TransUnion 2022 Global Digital Fraud Trends report—hints at a much larger trust landscape beyond retail and payments.

↑6.5%

Profile misrepresentation grew 6.5% between 2019 and 2021.

Personas vs. Identities

There are far more good guys than bad guys online. Yet, the malicious agents out there are good at capitalizing on breached and publicly available data to create a wide range of personas—and problems. This makes it difficult to know if an organization, social media profile or forum participant is who they say they are, or if they're real at all.

However, personas are not identities. Real people have real identities, and if you can determine the real identity behind a persona, you have much better data for deciding whether to trust them or not. If organizations can easily identify trusted customers, subscribers and users, they can achieve two goals. First, they can significantly reduce the costs associated with identifying and preventing fraud. At the same time, they can create a trusted digital environment where customers can interact with confidence and safety.

There are many areas where a trust-focused approach is becoming essential for enabling a seamless online experience.

Identity is at the core of trust. Traditionally, companies have adopted identity trust or verification strategies for specific use cases, such as approving credit-card transactions. For retail and commerce companies, identity verification is a mainstay of their fraud prevention programs. Yet, there are many other areas where a trust-focused approach is becoming essential for enabling a seamless online experience while thwarting hacked accounts, fake reviews, promo abuse and more. Understanding how this abuse occurs illustrates the impact of being able to identify trustworthy people.

Where Trust Can Have the Most Impact

Connected users interact across multiple online environments, from social media and online communities to marketplaces and gaming and streaming sites. Each time a person subscribes to a web service, logs onto a new site or engages in social media activity, they generate multiple identifying characteristics. These often include email addresses, usernames, mobile phone numbers, IP addresses and cookies. Social media users have an average of 8.4 different social network profiles, according to Finances Online.

In the wake of massive data breaches over the past few years, billions of identity records have become available for sale on the dark web. When you add up the sheer number of identity data sources available to exploit, it's pretty easy for bad actors to target large numbers of people for gain. And they do.

Fake Reviews Taint Online Marketplaces

Customer reviews are integral to marketplaces like eBay, Amazon and social media markets. Sites like Expedia also embed reviews for promoting destinations, while other sites' core purposes are to provide reviews and feedback. Even many small businesses include customer reviews on their websites. Fake online reviews have become a real trust problem because they're profitable. By definition, a fake review is any positive, neutral or negative review that is not an actual consumer's honest, impartial opinion and does not reflect a genuine experience of a product, service or business. According to Sift, 85% of consumers shopping online believe the reviews they read are sometimes, or often, fake or fraudulent[1].

How profitable are fake reviews? The World Economic Forum calculated that fake online reviews influence billions of dollars of ecommerce spending annually, $791 billion in the U.S. alone. For an unscrupulous business, buying fake positive reviews delivers immediate revenue benefits and boosts organic search rankings[2]. Purchasing fake negative reviews to post on competitors' sites have just the opposite effect. According to a UK reputation manager, just four negative reviews can cost a company 70% of its potential customers.

Four negative reviews can cost a company 70% of its potential customers.

Fake-reviews-as-a-service—delivering fake reviews from fake personas created using stolen or synthetic identities—have become widespread, with trading circles, commission structures and loyalty schemes. In other cases, fake reviews are used for extortion, with bad actors threatening that ecommerce sites' online ratings will drop if they don't meet payment demands[3].

$2.6K can buy a social media account with more than 300,000 followers

Online Communities—Anything Goes

Online communities, such as forums, news sites and websites for special interests heavily overlap with social media sites. Here, trust abuse practices include impersonation, imposter accounts and fake personas, fake news and deep fakes. The goal isn't necessarily financial. Instead, it might be to build followers, influence opinions or gather phishing targets for downstream fraud practices.

Impersonators typically copy photos, names, descriptions or hashtags from official accounts. They often create other accounts with names of random people and use them to "like" or post comments to the main imposter account. A 2017 report from Trend Micro

found that $2,600 can buy a social media account with more than 300,000 followers; $55,000 is enough to fund a Twitter attack that successfully discredits a journalist; and $400,000 can influence policy changes on trade agreements, impact elections or change the course of a referendum[4].

Deep fakes combine and superimpose existing images, video or audio onto source images or videos. According to the BBC, in 2019 the security firm Symantec reported three cases in which deep-faked audios of chief executives were used to influence financial controllers into transferring money. When the face and voice match, it's difficult for an unsuspecting employee to question the request.

Social Media: A Setup for Fraud

Social media is the setting for almost every imaginable form of fraud. The U.S. Federal Trade Commission said that in 2021, a quarter of fraud claims—95,000—came from social media with losses totaling $770 million[5]. The most common frauds involved romance, investment and bogus product scams. Fraudsters use social media sites to jump-start more advanced fraud schemes. More than one in four people who reported fraud in 2021 said it started on social media with an ad, a post or a message[6].

More than one in four people who reported fraud in 2021 said it started on social media.

With few identity verification controls in place, it's easy to manufacture fake social media personas or compromise existing profiles. This gives the fraudster "friends" to con and allows them to fine-tune their approach by studying the personal details that people share. In a major Facebook Messenger scam, fraudsters compromised Facebook accounts, logged in and used automated attacks to phish users' friends via the messaging app. The group used a technique to circumvent Facebook fraud detection, and the scam potentially affected hundreds of millions of Facebook users. That data has likely been resold and used to perpetrate advanced, lucrative forms of fraud.

The Unfair Fraud Advantage of Dating Sites

Even though lonely people have always been targeted by lowlifes and swindlers, online dating was turned upside down during the pandemic. Of the $770 million lost to social media fraud in 2021, a whopping $547 million was the result of romance scams. In 2020, Arkose Labs recorded four million attacks targeting dating apps. Most attacks on the dating platforms were focused on account takeovers that would be used for later phishing and scamming[7]. Other tactics include creating fake new accounts and profiles.

$547M

was lost to romance scams in 2021

Unlike other types of attacks, most of these are driven by sweatshop human labor instead of automation. Bots simply can't interact with users and respond to victims' messages. Almost all scams involve promises of significant financial gain through investments—complete with fake screenshots, websites, customer service agents and of course, fake products. In recent "pig butchering" schemes, crooks use dating apps or social media to build trust with lonely, vulnerable people for weeks or months before fleecing them through cryptocurrency trading. Once the victim authorizes payment to "invest," they're locked out of their "investment account" and the money and fraudster

are gone. Truly evil fraudsters record intimate conversations or videos and use these to blackmail the victim into paying money. In every case, a fake identity was mistaken by the victim as being a genuine person.

High Stakes on Gaming Sites

In 2020, online gaming was the most attacked industry, and in 2021 it experienced the largest percentage of annual fraud growth at 60% year over year. Significant growth in the gaming industry during the pandemic created a flood of new gamers. Fraudsters simply follow the money, barraging game platforms with bot attacks that target multiple touchpoints. Many online games feature sophisticated digital worlds with virtual economies that offer ways to make money, such as farming, reselling in-game gold and even trading real money. Gold farming was the top fraud type for gaming where in-game resources are harvested and sold for real money[8].

60%
year-over-year growth in online gaming fraud from 2020-2021

Other fraud attempts on gaming sites include policy violation through game abuses like gambling and collusion. Fraudsters abuse $0 authorization fee promotions to test credit cards, create fake accounts and hack existing accounts. Some players purchase virtual currency with stolen payment cards and sell the purchased items to others via marketplaces. False identities support all of these activities.

If only money was at stake. Online groomers are looking for different targets on online gaming platforms. They often use fake social media personas to target young people, sending out friend requests to see who responds. They “meet” targets in online forums and games, strike up conversations to build trust and then move the conversations to another platform or private chat. Multiple reports of grooming children online through Minecraft.net, Epic Games’ “Fortnite” and other game platforms have occurred in the EU and U.S.—some with tragic consequences.

More users don’t equal more accounts, which means substantial missed revenue for content platforms.

Streaming Services Subverted

Music, TV and other streaming content services offer numerous opportunities for fraud that hurt everyone involved—customers, artists and platforms. It starts with password-sharing. Streaming customers often share passwords, allowing family or friends to consume content from their account. More users don’t equal more accounts, which means substantial missed revenue for content platforms. In the case of Netflix, password-sharing has had a devastating impact. The company estimates that 100 million households worldwide—or one out of three households using its service—are streaming for free[9]. The company has lost 200,000 subscribers and its shares dropped 35% on the news.

Shared passwords also bypass account owner control, opening the door to malicious use. Credentials, credit card numbers and proprietary content are sold on the dark web. In 2020, Spotify customers reported that strangers were breaking into their family accounts. Not only did they freeload on subscriptions, they also gained access to family members' names and other data. It's more fodder for fake identities.

Fraudsters even make money on legitimate users' subscriptions. In one case, a crook stole and sold more than 200,000 customer account credentials for Netflix, HBO Max and Spotify Premium as part of an online service called AccountBot. Users of the site paid a subscription fee to obtain others' credentials for paid streaming services at a lower rate than the services charged.

The earlier that businesses can identify malicious account openings, the better they can protect themselves.

Forever a Target: Financial Services

Since the pandemic, financial services firms have been deluged with fake account applications based on stolen or synthetic identity data. Known as online account origination (OAO) fraud, this is a first step to launching all kinds of financial havoc. For example, credit fraud nets the fraudster credit or money they don't intend to pay back. Fake accounts are used to test credit cards before attempting to make fraudulent purchases. Rewards fraud siphons off reward dollars, points or miles. Sometimes the fraudster abuses free trials for products offered on subscription or promotions offering signup bonuses. Others "purchase" tickets online for an event, put them in the shopping cart and go to checkout where they use automation to stall checkout and force users to purchase the tickets at a higher rate from a broker. The earlier that businesses can identify malicious account openings, the better they can protect themselves from these types of fraud.

Fake investment scams also were a leading cause of fraud originating from social media platforms in 2021 with complaints increasing 168% year over year. This increase shows a dramatic increase in cryptocurrency investment scams fueled by social media[10].

168%

year-over-year increase in complaints of fake investment scams on social media from 2020-2021

Online Retail Fraud Continues

Let us count the ways that online retail and ecommerce fraud occurs. Identity theft, friendly fraud, chargebacks, return fraud and promotional fraud are the most typical. In 2021, online shopping fraud via social media sites became a leading cause of consumer fraud. Bogus products were advertised, enticing people to buy. Some ads impersonated legitimate online retailers and drove people to fake, but real-looking, sites. Not surprisingly, goods ordered were never received. Nine out of 10 times, this occurred on Facebook or Instagram.

Trust as a Strategic Weapon

The value of trust in online interaction is inestimable. When fraudsters' *modus operandi* are known, companies can leverage trust to their advantage. It begins with trusted identities. Organizations that can verify identities of their users—at any point, across all points and over time—can begin to identify trustworthy customers, followers and users.

What Does a Trusted Identity Look Like?

Although traditional identity verification (IDV) solutions can validate some customer attributes—street addresses, phone numbers or credit card numbers—these are no longer enough to establish trust. Much of that data is readily available on the dark web, so it does not necessarily mean that the person presenting it is actually who that data represents. Deeper insight into the data is required.

People continuously create digital data over time, and people who know each other leave digital traces of those connections. That's why seeing the connections between data points is so important. Fraud rarely occurs between people who know each other. Trusted identities verify connections between data and the person trying to access your site. They include the following characteristics:

- **Physical identity elements:** Traditional identifiers, such as name, address, phone number and credit card numbers
- **Online identifiers:** A person's digital footprints, such as email addresses, social usernames and online profiles
- **Density:** Data collected from multiple online and offline sources—confirmed and corroborated by multiple open source intelligence (OSINT) data sources from around the world
- **History and consistency:** Built over time, with logical reasons for adding new elements
- **Connections:** Identity elements connect to other people, organizations and places

Fraudsters can try to impersonate legitimate customers, but they can't create trusted identities. This is why trusted identities offer a safer approach to improving online trust and safety. A trusted identity solution should also automate data point correlation and trust scoring based on statistically significant data sets—presenting relevant data at a glance for fast, confident decision-making. Documented trust separates the bad actors and enables you to more easily prevent fake profiles, promo abuse, hacked accounts and other kinds of abusive or criminal attacks.

With trusted identities, organizations can give their customers and followers safe, frictionless online experiences.

Continuous adaptation enables you to verify a trusted digital identity at any point in the consumer journey. With trusted identities, organizations can give their customers and followers safe, frictionless online experiences—from the first visit through account setup and login to social interactions or transactions with your organization. This is especially true for online communities and social sites where trust is critical to building accounts and attracting new users. Trusted identities enable you to keep the door open while greatly reducing risk and exposure to fraud. The ability to continuously adapt keeps you current with changing threat landscapes, user demands and business models.

Finally, trusted identity information can be leveraged across your organization. It provides additional layers of protection for transaction, monitoring, sales, marketing, financial and cyber security efforts. You'll gain confidence for better decision-making and better data for fraud-defense systems.

It's Time for a New Approach

Digital trust and safety is shaping up to become a critical, revolutionary issue for online organizations, communities and everyday users. The online world depends on being able to move forward with trusted interactions, which are only possible when you know who is real and who isn't. The value of trust far outweighs the cost of fraud. Organizations that can successfully identify trust in online interactions will improve the customer experience and strengthen brand loyalty while extending customer lifetime value.

The value of trust far outweighs the cost of fraud.

Start With Trust

Pipl is the identity trust company. Our solutions enable organizations to identify trustworthy users, customers and followers so that they can enhance their digital trust and safety initiatives. We're ready to show you how to implement trust in the ways that matter most to your organization.

Contact us to learn more.

[1] Fake Reviews: A Growing Fraud Concern Affecting Brand Loyalty and Growth, Sift, 2019

[2,3] The Economic Cost of Bad Actors on the Internet Fake Online Reviews 2021, Cheq

[4] Lion Gu, Vladimir Kropotov & Fyodor Yarochkin, Fake News and Cyber Propaganda: The Use And Abuse of Social Media, Trend Micro, June 13, 2017

[5] How to Stay Safe from Scammers Sliding into Your DMs, Forbes Advisor, Feb. 10, 2022

[6] Social media a gold mine for scammers in 2021, Federal Trade Commission, Jan. 25, 2022

[7] Broken Hearts, Stolen Wallets: The Steady Stream of Fraud on Digital Dating Platforms, Security Boulevard, Feb. 11, 2021

[8] Gaming sees largest US annual digital fraud growth in 2021 at 60% YOY, Online Gambling Daily, March, 2022

[9] As Shares Plunge, Netflix Takes Aim at Password Sharing, Ads, US News, April 21, 2022

[10] Top Ten Scams, Fraud!Org, Feb. 2022

ABOUT PIPL

Pipl is the identity trust company. We make sure no one pretends to be you. We use multivariate linking to establish deep connections among more than 330 billion trust signals—email, mobile phone and social media data that spans the globe—and then look at the big picture to derive identity trust. Our solutions allow organizations to provide frictionless customer experiences and approve more transactions with greater confidence and speed. **Learn more at pipl.com.**

pipl®