pipl

Start Reducing False Declines in 4 steps

Fraud prevention measures

The bad news for e-commerce merchants, consumers, and financial service providers is that losses from e-commerce fraud are projected to hit $6.4 billion in 2021. But wait, it gets worse. Losses from false declines will likely reach $443 billion—almost 70 times more. Does this mean merchants' and financial institutions' fraud prevention measures are more harmful than the original problem?

Well, it's not that simple. Global retail e-commerce sales exploded because of the pandemic and will hit $4.9 trillion in 2021 on their way to $6.5 trillion by 2023. As e-commerce sales increase, so does fraud. Throw in extremely complex payment processing and settlement channels and it becomes very difficult to quickly sort out fraudsters from legitimate customers. However, preventing fraud and false declines depends on the quality of your data. There are four elements essential to transaction review decisions for helping reduce false declines.

E-commerce fraud losses are projected to total **$6.4 billion** in 2021.

What triggers false declines?

False declines, also known as false positives, are those cases when a payment processor or customer's card-issuing bank incorrectly rejects legitimate customer transactions. As many as 62% of surveyed merchants reported their false decline rates had increased between 2017 and 2019.

Declines happen for many reasons. Payment processor network outages can cause customer transactions to be declined. In February, 2021, a payment provider network outage caused problems for customers at restaurants and stores including McDonald's, Ikea, Forever 21, and government agencies across the country. Assuming that networks are up and running, there are at least four other reasons why a legitimate transaction might be declined.

Overseas IP Addresses

Orders coming from outside-of-the-country IP addresses are often viewed suspiciously and with good reason. Large cybercrime rings operate out of Asia and there are high rates of fraud across European countries. But individuals who travel or work overseas often purchase products online and have them shipped back home, which can raise suspicion.

Employer VPNs

The pandemic forced a migration of employees from offices to their homes. This resulted in high volumes of business network traffic coming from homes into corporate offices over encrypted VPN connections designed to protect company data. However, VPNs by nature mask the user's IP address, and they can often display an IP address originating in a foreign country, depending on where the VPN servers are located.

Breached Data

With billions of compromised records out in the open from data breaches, identity elements can easily end up on blacklists. Therefore, it's not hard to see how an email address, phone number, and other personal details can be used both by their legitimate owners and by fraudsters.

New Accounts

A report from Forter finds that new shoppers are five to seven times more likely to have their purchase declined than returning users. Known as New User Missed Opportunities (NUMOs), rejection of first-time checkouts can cost retailers big.

The Impact is Staggering

The first, most obvious impact of false declines is lost revenues. The higher the price tag, the more likely the transaction will be declined. In its 2017 Global Fraud Survey, the Merchant Risk Council reported that the average online store declined 2.6% of all incoming orders because of fraud concerns, including declining 3.1% of all orders valued over $100. Currently, according to the Forter report, immediate annual revenue losses range from $798 per customer for home and garden purchases to $930 per customer for apparel and accessories and $1062 per customer for food and beverage sales. Not only do retailers lose immediate revenue, they also lose their investments in activities designed to attract, convert, and retain customers.

3.1% of all orders over $100 are declined due to fraud concerns

The High Cost of Dissatisfaction

A declined customer can be frustrated at best—and vengeful at worst. Customers can spend hours of valuable time researching product options, comparing prices, and making their decisions. By the time they click the Buy button, they've also had to hand over a significant amount of personal information. When their transaction is declined, it's not surprising that 40% of declined users will never try that merchant site again.

Worse, declined customers will tell others about their experience. American Express found that consumers tell an average of 11 people about their good experiences and 15 people about the bad ones. If they take their frustration to social media channels, the fallout and bad reviews can cause substantial brand damage to the merchant—regardless of the reason for the decline.

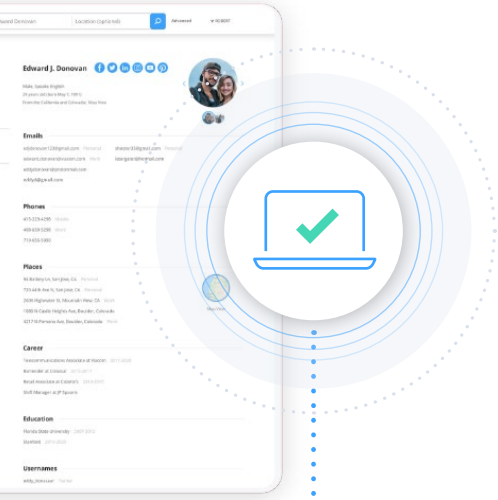
Corrupted Automated Systems

Data generated from payment transactions can be artificially skewed by high false positive rates. When this data is fed back into automated decision support systems, it can corrupt business rules, leading to incorrect assumptions.

Suppose your system analyzes 100 transactions and identifies 20 as risky. After review, you find that 10 are truly fraudsters but 10 were false positives. Of the 10 false positives, five might contact your customer support team, allowing you to resolve the problem and correctly verify the transaction. But the others silently slip to a competitor. The five false positives are never identified by the system as false, resulting in the anti-fraud detection tool calculating risk with flawed data analytics, which can further reduce its accuracy.

Four Ways to Reduce False Declines and Loss

So how can you make more good decisions and reduce loss at the same time?
After all, merchants shouldn't have to sacrifice revenue for customer satisfaction—or vice versa. As we mentioned before, good prevention of fraud and false declines depends on good data. Here are four ways that better data delivers better results.



1
Increase Data Completeness

More—and more relevant—data delivers a more comprehensive picture of the customer. When creating an account, customers only provide the data they want you to have. They are likely to have additional phone numbers or email addresses that you don't know about. Traditional identity database sources often lack online identity detail. Go beyond standard account information with access to high-confidence email, mobile, and social data. These details also frequently uncover additional elements—such as a second mobile phone number or email address—that can help you verify the customer.

Online identity details can be automatically scored to assess their level of trustworthiness. Pipl uncovers—and assigns an integrity score—to show connections between the customer and other people for a more complete picture of the person behind a transaction. This is especially useful for thin-file customers, who might also be first-time account openers. Having access to the largest collection of global online identities makes it faster and easier to verify identities when confronted by overseas IP addresses or transactions from outside the U.S.

2
Detect Synthetic Identities

Synthetic identity fraud is one of the fastest-growing financial crimes in the U.S., costing financial institutions more than $6 billion a year. Fraudsters combine legitimate data, such as a Social Security number, with fictitious information—or create a completely fake identity and apply for a new account.

It's at this point where banking, lending, and retailers must look past the individual identity to analyze its connections and relationships to other individuals and characteristics. Often, information that you would expect to appear, doesn't. Several identity elements look to have been created at the same time, which is not the case with most real individuals. Or there appear to be random connections that don't make sense. Pipl identifies synthetic identities based on what's there—and what's not—giving reviewers confidence in their decisions to correctly decline new fraudulent accounts or transactions.

3

Increase Accuracy

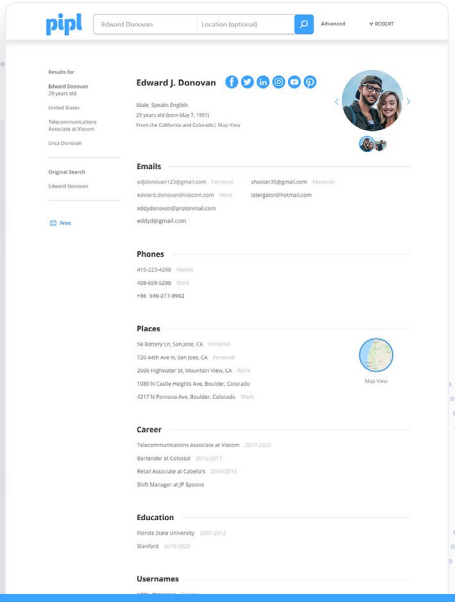
Financial organizations increasingly need identities to be verified using 2+2 verification. This means that at least two identity elements must match across at least two different sources. With global reach and data from hundreds of public data sources, Pipl automatically connects and verifies multiple identity elements from multiple sources. Choose phone-to-physical address connections; phone-to-email connections; or other combinations as needed.

Including global email, mobile, and social data and automatic 2+2 verification capabilities improves data analytics quality in decision engines as well. You can continuously improve policies and rule sets to further reduce customer friction and loss.

4

Accelerate Decision Speed

Visual representation of identity elements, connections, and confidence levels between them provides a big-picture view of the person behind the transaction and at-a-glance insight. Pipl scores each identity element and connection according to its accuracy and completeness so reviewers can trust what they see.



Putting It All Together

Data completeness, an ability to detect synthetic identity, 2+2 verification capabilities, and accelerated decision-making go a long way toward helping reduce false declines. Combine these elements of a strong identity verification platform with access to more than 3 billion trusted identity profiles and proactively begin to reduce false declines and loss. For more information, visit Pipl Identity Verification & Fraud Prevention.

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.