



Holiday Season

The Prime Time for ID Thieves and
Financial Criminals

What's Inside

Summary	02
The Global Picture	03
An Overview of 2020 and Reasons Behind the Rise in Fraud	05
Covid-19 Contribution to the Rise in ID Fraud	06
Major Fraud Threats to Look Out for this Holiday Season	08
Impersonation Attacks	08
Item-not-received Fraud	09
Chargeback Fraud	09
Account Takeover Fraud	09
New Account Fraud	10
Credit Card Fraud	10
Predictions for Holiday Season 2021	11
Responding to the Rising Fraud Threats with Artificial Intelligence	12
Know Your Customer	12
NFC Verification	13
Facial Biometric Authentication	13
Consent Verification	14
Address Verification	15
Conclusion	16

Summary

The most awaited time of the year faces the highest number of fraud attempts. From chargebacks to account takeover, almost every kind of criminal activity is at its peak during the holiday season. While everybody is planning the epic break from everyday drama, perpetrators are plotting against consumers and businesses.



In 2020 alone, the holiday season encountered a 20.55% fraud rate, whereas the rate between January and October was 16.63%.^[1]

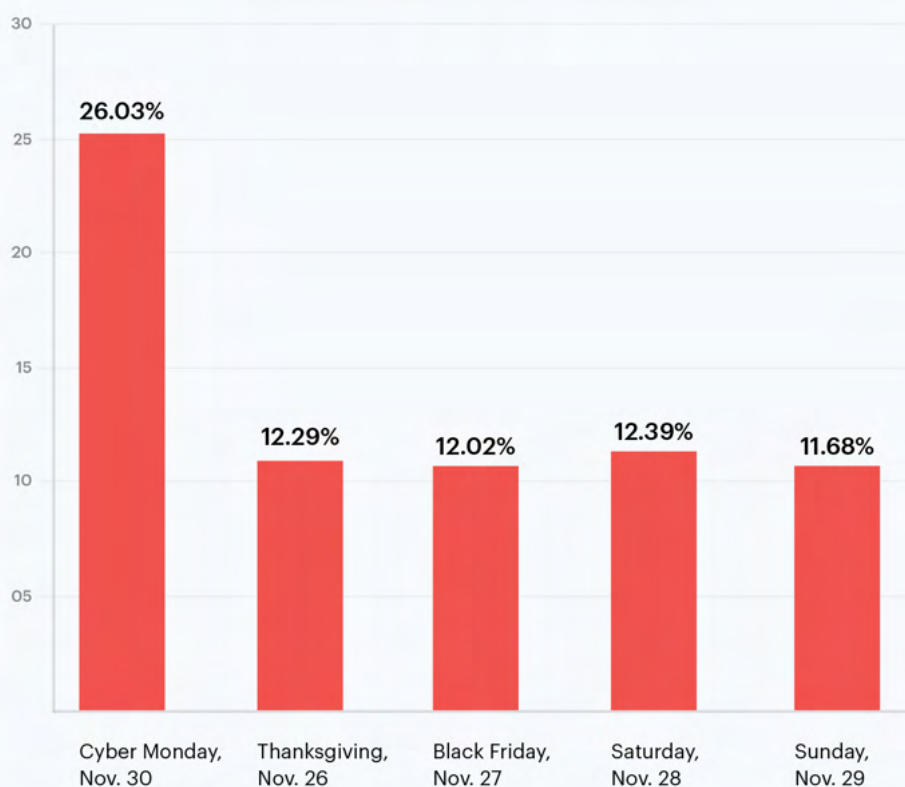
Based on the facts and statistics of the last five years, our experts are predicting a sharp increase in holiday season fraud. Due to the Covid-19 pandemic, the finance sector, retail industry, and online shopping sector must be prepared to face rising numbers of false chargebacks and manipulated financial information.



The Global Picture

The corporate sector across the globe has experienced a remarkable increase in criminal activities. Advanced technology is no longer restricted to businesses, but fraudsters are strategically employing artificial intelligence and machine learning algorithms to manipulate identity documents and use them for their illicit plans. Halloween, Black Friday, and Cyber Monday create opportunities for identity and financial crime worldwide. As we move ahead, bad actors extend their activities to Thanksgiving, Christmas, New Year's Eve, and New Year's Day.

Holiday Season **Fraud** Rate in **2020** by Events



Source: TransUnion



Did you know the average daily rate for payment fraud was 117% higher than 2019 in the United Kingdom last year?^[2]

Given the circumstances, the **Federal Trade Commission (FTC)** issued a report warning older adults of the rising threat of frauds. The report further revealed that online retailers are on the brink of chargebacks and that the pandemic is partly to blame in this situation.

The holiday season is right around the corner, government bodies in all regions of the world are educating businesses and individuals to steer clear of perpetrators this year as the threat of fraud is significantly high in 2021.

Hovering back to the fraud statistics of 2020 by Shufti Pro, Asia, Africa, the Caribbean, and the USA had the highest rate of identity fraud.

In another section of the report, the FTC stated that romance scams garnered the largest dollar loss of \$139 million in 2020, a 66% increase from 2019.

Regions with the Highest Rate of ID Fraud in 2020



An Overview of 2020 and Reasons Behind the Rise in Fraud

The year 2020 was all about lockdowns, new restrictions, Covid-19 SOPs, and acclimating with the new normal. While everybody was trying to cope with the deteriorating situation, bad actors came up with many new techniques to manipulate businesses. According to Shufti Pro's findings, identity fraud increased by a whopping 3.36% in 2020. Not just this, we captured a rise in biometric fraud attempts as well. Digital replay attacks and various spoof attacks were repeatedly captured by our face verification. Out of all the face verifications performed in 2020, 22.44% of them failed due to biometric fraud attempts.

Why are businesses experiencing a rapid increase in fraud attempts anyway? Out of the many reasons Shufti Pro's experts have shared, here are the top four reasons behind the increase in criminal activities.



Lack of robust identity screening services during client onboarding



Businesses often compromise ID verification for the sake of enhancing customer experience



Loopholes in the regulatory framework for some sectors like real estate become a profitable outlet for perpetrators



Strategically advanced techniques from fraudsters to dodge screening

Covid-19 Contribution to the Rise in ID Fraud

The coronavirus outbreak resulted in a number of opportunities for businesses and fraudsters alike. While many new business ideas surrounded us, imposters also benefited from the unpredictable situation. A report revealed that global losses from fraud have tripled to USD 32.39 billion in 2020 from USD 9.84 billion in 2011. Furthermore, the losses are expected to exceed \$40 billion by the end of 2027.^[3]

“

“As a tech enthusiast and identity verification expert, I have seen fraudsters adapt with all the new trends in the blink of an eye. They are, by far, the most opportunistic people I have come across and this time, it's the pandemic that has given them an edge”

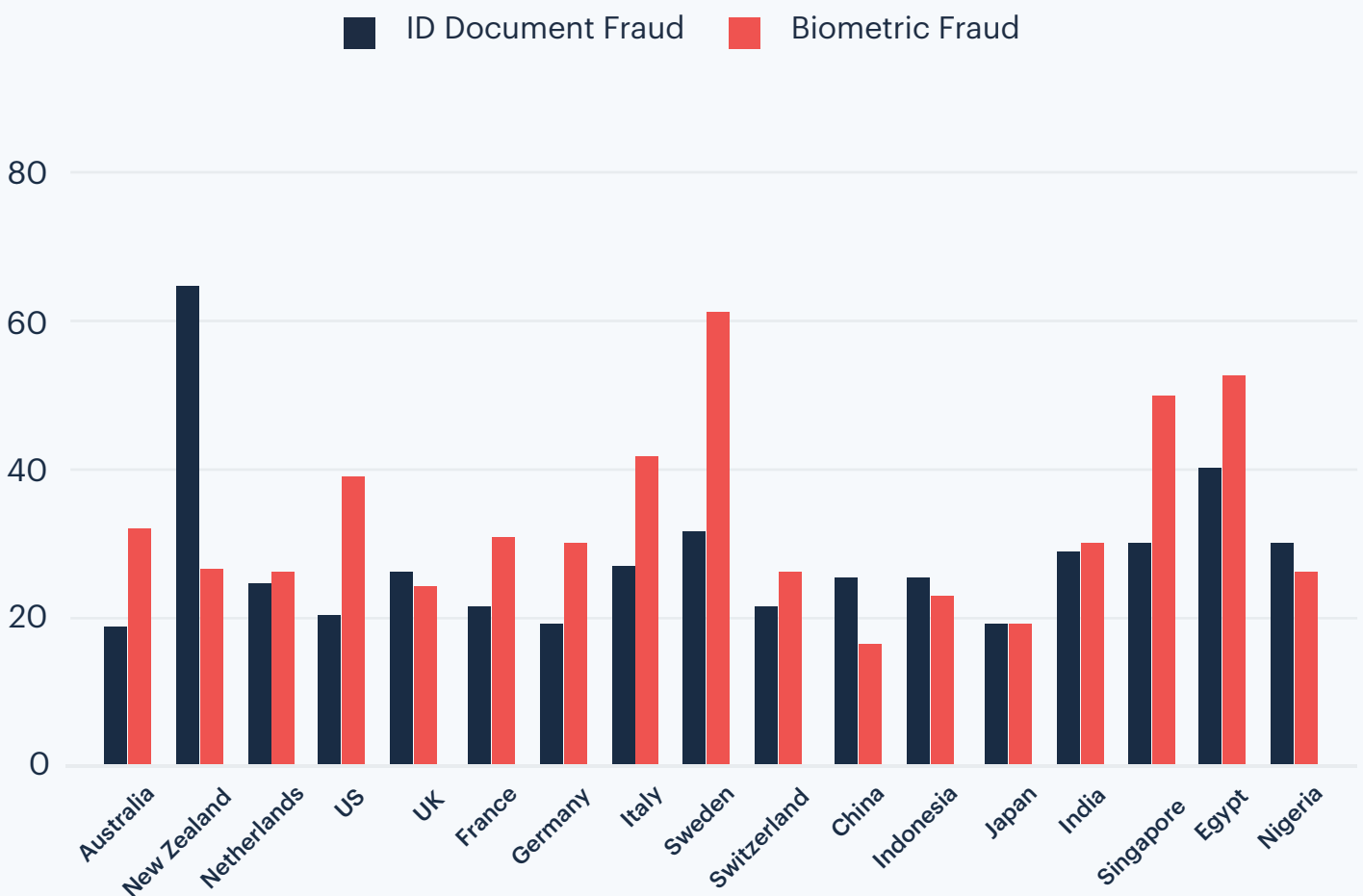


**- Shahid Hanif,
the Co-founder and
CTO of Shufti Pro.**



According to Shufti Pro’s Global Identity Fraud Report 2020, fraud rate during the pandemic was 3.36% up and the following countries had the highest identity fraud rate:

ID Fraud During the Pandemic



Major Fraud Threats to Look Out for this Holiday Season

This holiday season will stand out for everyone. eCommerce businesses are ready to enjoy skyrocketing online purchases and consumers are planning to enjoy the perfect holiday season sales. However, fraudsters are making all possible efforts to steal identities and misuse Personally Identifiable Information (PII) for their illicit activities. Not just this, but all online retailers are at stake since the strategically strong imposters are making their next move to manipulate businesses.

Holiday Season Fraud Rate in 2019 and 2020

	2019 (in %)	2020 (in %)
Jan - Oct	19.91	20.83
Nov - Dec	29.90	21.51

Between January and October 2021, Shufti Pro has encountered an increase in identity fraud. Given the increase in fraud attempts, this year's holiday season will witness a sharp rise in fraudulent activities.

Considering the past trends and this year's fraudulent activities, here are some of the frauds that Shufti Pro's experts are predicting to increase in 2021.

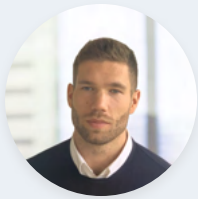
Impersonation Attacks

Enhanced technology has benefited everyone, including bad actors. Over time, they switched from document fraud to more sophisticated forms of criminal activities. Biometric frauds grew significantly in 2020 and digital replay attacks, 2D and 3D spoof attacks were

repeatedly encountered during identity verification.

“

Cybercrimes doubled in 2020 and without a sound approach to fight identity fraud, it is nearly impossible to combat perpetrators this holiday season. To secure businesses from million-dollar worth of identity and financial fraud, every sector is in dire need of AI-backed solutions



- **Victor Fredung**,
the **CEO of Shufti Pro**

Item-not-received Fraud

Getting monetary benefit without actually buying a product is what imposters seek. The holiday season being the prime time for fraudulent activities, imposters will be filing false claims to get a refund under “item not received” complaints. All eCommerce platforms must be prepared to identify fraudulent claims before they lose a large amount of money to scammers.

Chargeback Fraud

One of the oldest techniques in the book, yet the most commonly used by imposters. According to a report^[4], around 30% of the chargebacks are initiated as a result of stolen credit cards. This year, online transactions have more than doubled. Henceforth, experts are predicting a significant increase in chargeback fraud this year.

Account Takeover Fraud

Taking over someone else’s account and conducting fraudulent transactions has been a problem for over a decade. Mobile banking, e-wallets, and widespread crypto adoption is opening gates for perpetrators to execute their illicit plans. In 2020, a 282% surge in fraudulent logins was encountered. Reports reveal that e-commerce sales are estimated to reach \$206.88 billion during the holiday season (11.3% higher than 2020)^[5]. Imposters have a great opportunity to leverage account takeovers to take advantage of more online shoppers.

^[4] Chargeback Fraud Statistics

^[5] eCommerce Sales in 2021

New Account Fraud

New account fraud is among the toughest illicit activities to identify because scammers use synthetic identities that have never been used for fraud before. New accounts are being opened under victim's names and this time, data breaches soared skyhigh. According to Fortune, the reported data breaches have already exceeded 2020's cases by a whopping ^[6]17%. This means bad actors have a lot of data in 2021 to create synthetic identities and commit new account fraud.

Credit Card Fraud

The Federal Trade Commission (FTC) report ^[7]reveals that more than 130,000 credit card fraud complaints have been filed since the second half of 2020 and consumers have lost around \$182 million to this fraud. Banks are at a higher risk of credit card fraud attempts this year and the only way out is ensuring legitimacy of the transaction information shared by the end-user with the financial institution.



[6] Reported Data Breaches in 2021

[7] FTC Report

Predictions for Holiday Season 2021

Based on facts and statistics, Shufti Pro's experts have suggested the following:



More Digital Buyers = More Fraud

As of this year, there are 2.14 billion digital buyers worldwide ^[8] giving bad actors a great chance to acquire unauthorized access to accounts, commit friendly fraud, and several other crimes.



Higher Customer Expectations

With massive digital adoption, customers are expecting more convenience from online businesses. As firms seek to enhance customer experience in the digital space, there is a high probability that they might compromise on anti-fraud systems and onboard fraudsters.



Large Transaction Volume

Since digital buyers have increased, the online transaction volume has tripled in 2021 with payments projected to reach USD 6,752,388 million in 2021. ^[9] That being said, imposters have a wider area to bank on for their illicit plans. Moreover, higher transaction volume can lead to failure of fraud prevention systems.



Lack of Robust Fraud Prevention Measures

Lastly, lack of robust identity screening solutions is another contributor to the rise in ID fraud. Without IDV and fraud prevention protocols, businesses must prepare themselves for more financial losses, damaged reputations, and non-compliance penalties.

^[8] Digital Buyers Worldwide - Statista

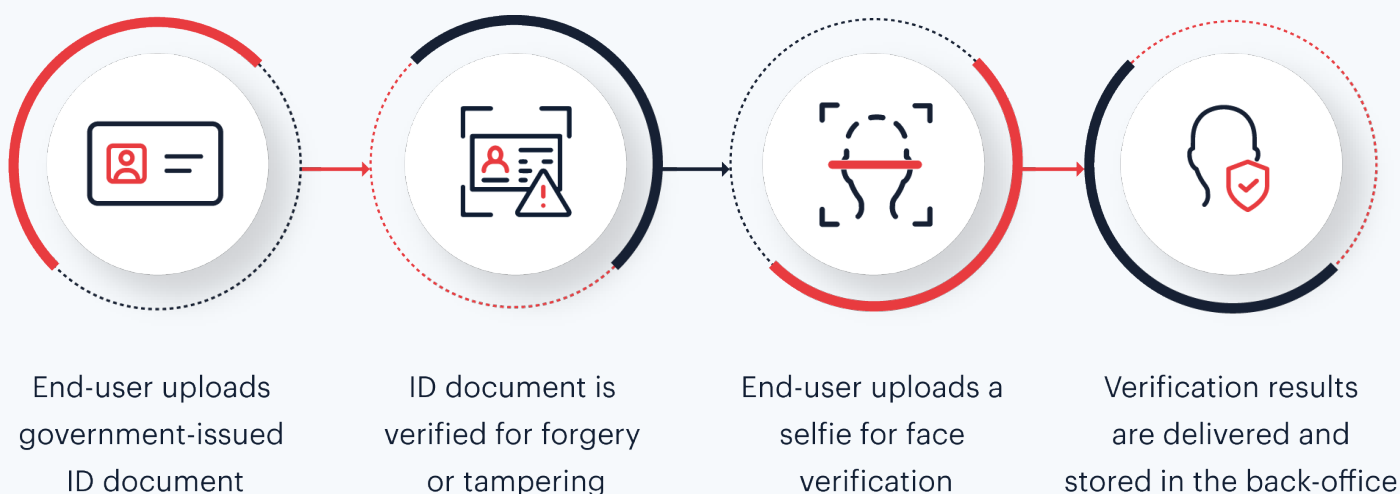
^[9] Digital Payments in 2021 - Statista

Responding to the Rising Fraud Threats with Artificial Intelligence

The rising number of criminal activities and predicting scams for the holiday season can be prevented with a bunch of AI-driven solutions. Shufti Pro has a wide array of options that satisfy the identity verification and screening needs of businesses in any industry. From the finance sector to the eCommerce industry, we provide solutions to everyone. Given the current scenarios, here are the top five ways to combat criminal activities during the holiday season:

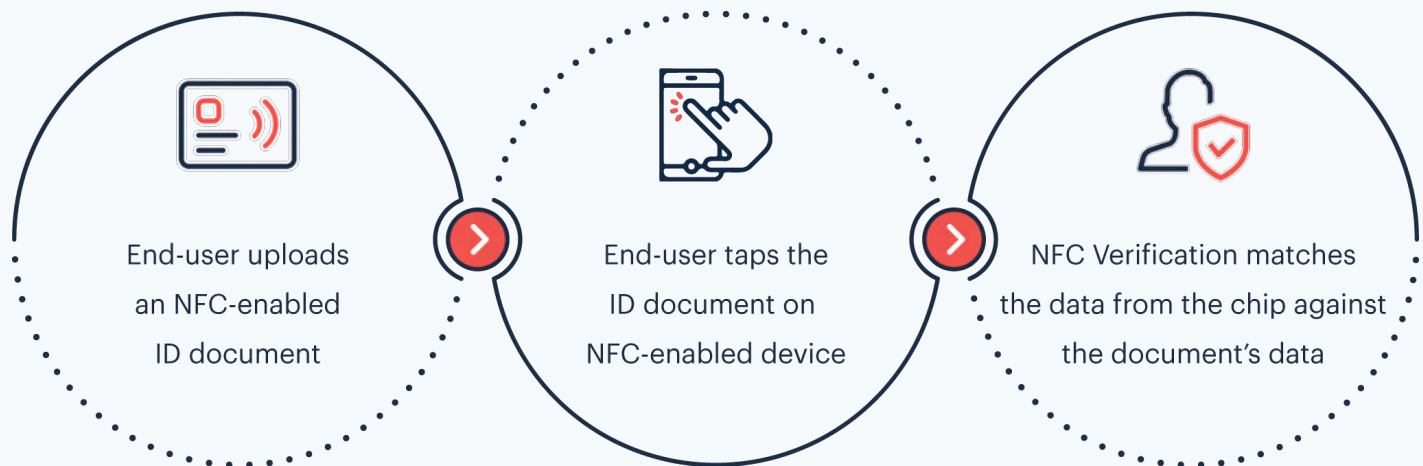
Know Your Customer

AI-driven identity verification service lets businesses onboard legitimate customers in seconds. Before confirming a transaction, verifying the identities of prospects gives companies an edge over imposters. You can ensure that the person is actually who they claim to be. With Shufti Pro, you can verify identities in more than 150 languages and 3000+ identity document types. Moreover, the verification results are 98.67% accurate and stored in the back-office for future case building.



NFC Verification

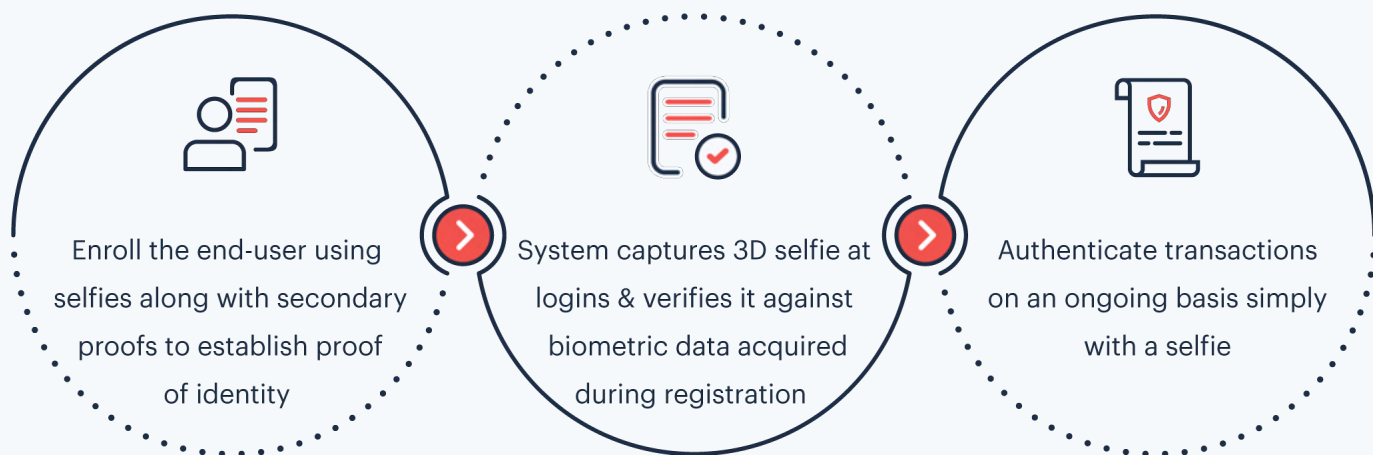
According to PwC, a 42% increase in cashless payments can be expected by the end of 2025, whereas 89% of the respondents agreed to the shift towards e-commerce would continue to increase.^[10] With the mass adoption of cashless methods of transactions, **NFC-based identity verification** is among the most reliable solutions businesses could ask for. PII encrypted in chip-based identity documents is hard to mess with and so, verifying NFC-based ID documents is a better choice. The accuracy of verification results is higher and only a tap of the document is required for verification.



Facial Biometric Authentication

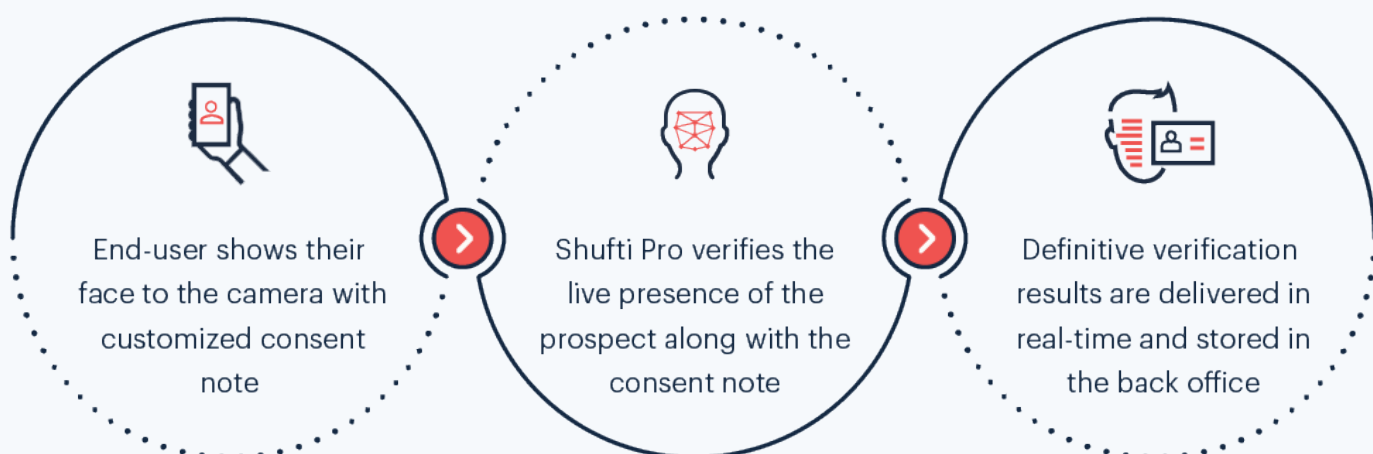
Unauthorized access to accounts can now be prevented with selfie login. **Facial Biometric Authentication** requires every account holder to login using a selfie. Since there is no concept of saved passwords here, facial biometric authentication at login serves as a strong defense mechanism against perpetrators. And that's not all, businesses can perform ongoing KYC and maintain updated customer profiles.

^[10] Payments in 2025 and Beyond



Consent Verification

eCommerce platforms can prevent the rising chargeback frauds this year with **Consent Verification**. Get your end-user's approval before a purchase and avoid hefty financial losses due to friendly fraud. Consent verification lets you ensure the live presence of the end-user and confirm the purchase for a legitimate entity.



Address Verification

Receiving complaints for delivering to the wrong address? Avoid the mess this holiday season with [Address Verification](#). The simple 3-step process allows businesses to run a risk-free business with legit customers.



Conclusion

To sum up, the digital space is now more prone to criminal activities than ever. Covid-19, advanced technology, and numerous other reasons have contributed to the rise in identity fraud. However, businesses can opt for AI-powered solutions to combat the surging fraudulent attempts. Shufti Pro's state-of-the-art identity verification solutions allow businesses to verify clients in seconds and 98.67% accurate results make legit customer onboarding easier.



Learn more about the holiday season frauds and
how you can combat them from our experts

Contact Us

Or try our services for free for seven days

Get Free Trial

www.shuftipro.com

 sales@shuftipro.com



Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.

Disclaimer: No warranty or claim is herein provided that information contained in this document is accurate, up-to-date, and/or complete. All information provided in this document is limited for general informational purposes only. In no circumstance(s), does such information constitute as legal or any other advice. Any individual or company who intends to use, rely, pass-on, or re-publish the information contained herein in any way is solely responsible for the same and any likely outcomes. Any individual or company may verify the information and/or obtain expert advice independently if required.