



# 2019

HOLIDAY NEW ACCOUNT

**FRAUD REPORT**



Jumio's Annual Global Look at Online Identity Fraud  
from Black Friday to Cyber Monday

**JUMIO**<sup>®</sup>

# BACKGROUND

It's become a holiday tradition: shoppers bombard retail stores to take advantage of holiday sales on Black Friday, then retreat to their computers to shop for bargains online on Cyber Monday. But this sales phenomenon is not limited to the United States anymore. Retailers across the globe are participating in Black Friday and Cyber Monday sales by offering deep discounts to shoppers, whether they're shopping at the mall or from their own couch with a smartphone.

In Europe, more than half of holiday purchases were made online, according to [PwC data](#), while South Africa topped the list of most online searches for Black Friday this year (according to Google data). In Argentina, Black Friday sales grew more than 376% in the past five years, according to a [survey](#) by Black Friday Global — even though the country doesn't technically celebrate this retail tradition.

Unsurprisingly, this growth has attracted cybercriminals.

Much of the attention has been on fraudulent transactions and bogus chargebacks. A new study from [iovation](#) shows a 29% increase in suspected online retail fraud during the start of the 2019 holiday shopping season compared to the same period in 2018, and a 60% increase over the same period from 2017 to 2019. These findings are based on the online retail transactions analyzed for e-commerce customers between Thanksgiving and Cyber Monday over the last three years. The top days for transactions are Black Friday, with 26% of legitimate holiday weekend transactions and 25% of suspected fraudulent transactions, and Cyber Monday, with 22% of legitimate transactions and 21% suspected fraudulent.




**29%**

increase in suspected  
online retail fraud

# THE IMPACT OF DATA BREACHES AND THE DARK WEB

It's difficult to attribute the reasons for the increase, but new account fraud, account takeovers and identity theft have all experienced double-digit increases in 2019. Presumably, some of this increase is being fueled by massive data breaches, including:

<b>VERIFICATIONS.IO</b>	<b>FIRST AMERICAN FINANCIAL</b>	<b>COLLECTION #1</b>
<p> <b>Date reported:</b> March 7, 2019</p> <p> <b>Impact:</b> 800 million to 2 billion records worldwide</p>	<p> <b>Date reported:</b> May 25, 2019</p> <p> <b>Impact:</b> About 885 million files related to mortgage deals</p>	<p> <b>Date reported:</b> Jan. 17, 2019</p> <p> <b>Impact:</b> Nearly 773 million unique email addresses and more than 22 million unique passwords</p>
<b>FACEBOOK</b>	<b>FORTNITE</b>	<b>ELASTICSEARCH CLOUD STORAGE</b>
<p> <b>Date reported:</b> April 3, 2019</p> <p> <b>Impact:</b> More than 540 million records exposed</p>	<p> <b>Date reported:</b> Jan. 16, 2019</p> <p> <b>Impact:</b> About 200 million gamers worldwide</p>	<p> <b>Date reported:</b> Jan. 21, 2019</p> <p> <b>Impact:</b> 108 million betting records</p>

Much of the data from these breaches ultimately finds a home on the dark web where the information can be bought and sold. For example, you can buy a passport scan on the dark web for the average price of \$14.71. The price goes up with proof of identification. In fact, it's common for both counterfeit and legitimate scans to come with various forms of identification: a selfie, utility bill, and/or a driver's license, for example. If proof of ID is added to a passport scan, the average price jumps from \$14.71 to \$61.27.

These large-scale data breaches are also fueling identity theft and the creation of fake accounts. Unfortunately, traditional methods of identity verification, including credit bureau pings and knowledge-based verification, do not assess whether the person supplying the identity information is the actual person they are purporting to be. As more online enterprises adopt biometric-based identity verification solutions that leverage a government-issued ID (e.g., driver's license) and a corroborating selfie, the market for these counterfeit items on the dark web has increased.

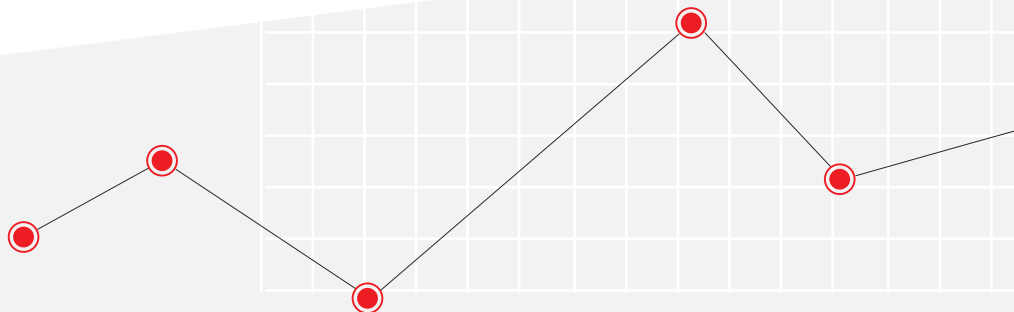
# JUMIO'S 2019 HOLIDAY NEW ACCOUNT FRAUD REPORT

Fraud takes many forms. Jumio's Holiday New Account Fraud Report examines fraud patterns between Black Friday and Cyber Monday when new online accounts are created. The report analyzes millions of identity verification transactions around the globe to determine if the commercial fraud trends that impact retailers are also evident when new accounts are being created.

It's important to understand that the first step in identity theft often starts with new account creation. Identity theft is the deliberate use of someone else's identity (e.g., name, address, Social Security number, bank accounts) to get money and credit and make holiday purchases. But, identity theft is obviously being used for money laundering, to perpetrate online fraud, steal property, falsify educational and other credentials, access healthcare and more.

When users create new accounts, whether for a banking account, sharing economy account or online gaming account, some portion of those accounts are fraudulent. In Jumio's 2019 Holiday New Account Fraud Report, we track ID fraud patterns across time, regions and industries to spot material trends.

## THE DATA



The data used in this report has been aggregated and anonymized across all of Jumio's customers from 2014 to 2019, specifically for the holiday period of time between Black Friday and Cyber Monday. In this third edition of Jumio's Holiday New Account Fraud Report, attempted fraud is defined as an attempt by an individual to create a new online account by manipulating a government-issued ID. The company compared ID fraud patterns from millions of ID verification transactions between 2014 and 2019 across various industries, focusing on the period between Black Friday and Cyber Monday, including the day before and the day after this timeframe (Thanksgiving and the Tuesday after Cyber Monday).

**1M+**

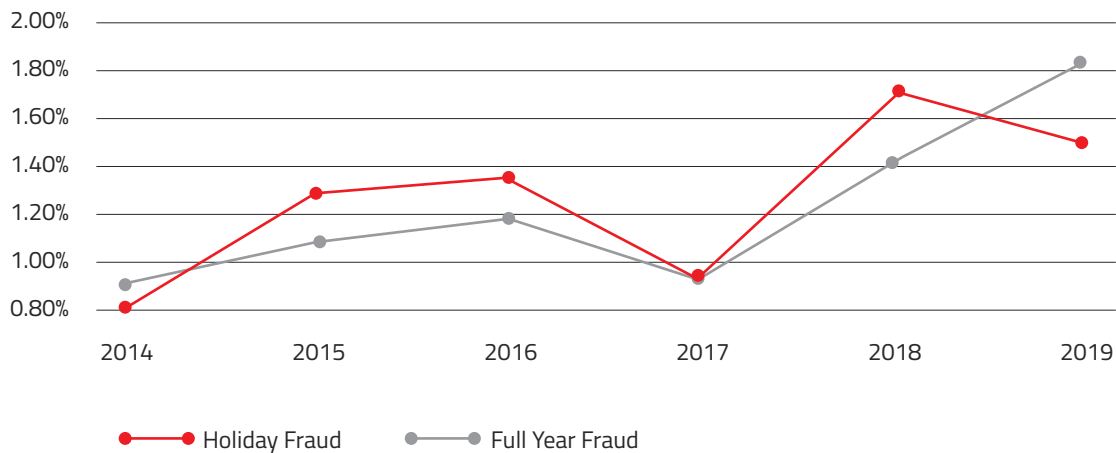
verification  
transactions

**The data in the 2019 report stems from more than one million ID verification transactions across a broad range of industries including banking, cryptocurrency exchanges, online gaming, insurance, travel, sharing economy, e-commerce and online services.**

# ID FRAUD DURING THE HOLIDAYS VS. FULL YEAR

One of the more interesting findings from this year's analysis is that fraud levels during the holiday period were actually less than the full-year average. In fact, fraud levels were 19% less during the extended holiday weekend than the rest of the year. Holiday new account fraud was also down 13% from holiday 2018 levels. Over the last six years, there is not a clear pattern that suggests online ID fraud (at account creation) is materially higher during the holiday week than during other parts of the year. But, there has been a steady rise in full-year and holiday fraud over the past six years — with 2017 being the only year when fraud rates dipped.

**HOLIDAY AND FULL YEAR FRAUD 2014-2019**



# FRAUD PATTERNS BY REGION

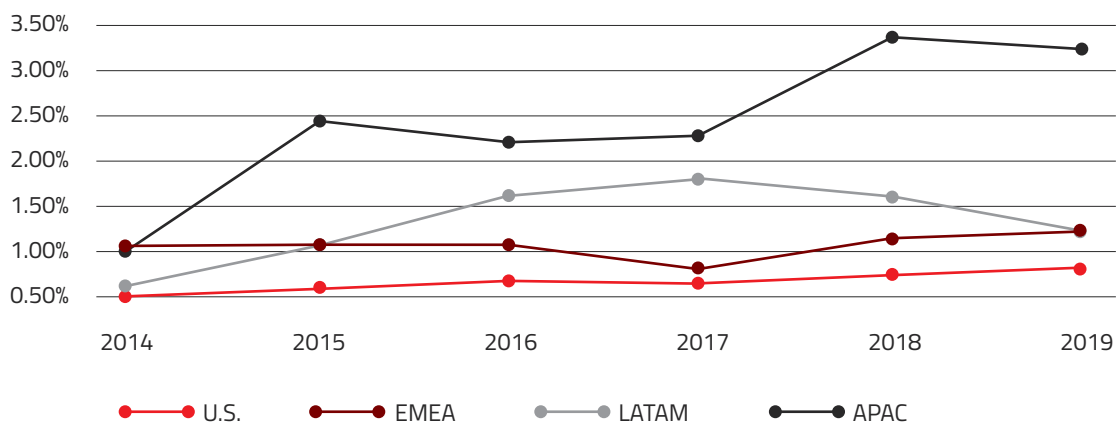
On a global basis, full-year fraud rates increased 28% in 2019 year-over-year (vs. 2018 levels) and 96% over 2017 levels. The Asia-Pacific region experienced the highest rates of fraud at 3.27% while the U.S. had the lowest rates of fraud at 0.88% — a trend which has been pretty consistent over the last six years.

There are a number of contributing factors to help explain the fraud levels in Asia-Pacific. The rapid pace of digital adoption and a correspondingly fast-growing digital ecosystem are changing the relationship between businesses and consumers in the region. The threat from online and mobile fraud is growing in the region, with digital financial services firms in China, Hong Kong and Indonesia now among the least trusted by consumers (source: Experian, 2019 Global Identity and Fraud Report, May 2019). Fraud cases were most commonly reported during retail banking activities, especially when customers used their cards, the report said, but instances also grew in the consumer tech, digital-only, telecoms and airline sectors.

## Full-Year ID Fraud Rates by Region

The chart below depicts the growth rates by region from 2014 to 2019. As a region, Asia-Pacific (APAC) has the highest levels of fraud in part because of the high fraud levels in specific countries (e.g., Indonesia). More mature markets, including the U.S. and EMEA, have also experienced increasing new account fraud levels over the last three years, while fraud rates in Latin America have started to decline.

**FULL YEAR ID FRAUD RATES BY REGION**



Region	2014	2015	2016	2017	2018	2019	YoY Change
U.S.	0.53%	0.57%	0.65%	0.62%	0.66%	0.88%	33.7%
EMEA	1.05%	1.08%	1.08%	0.74%	1.17%	1.30%	11.8%
LATAM	0.63%	1.07%	1.70%	1.83%	1.62%	1.31%	-19.1%
APAC	0.98%	2.47%	2.21%	2.32%	3.35%	3.27%	-2.3%
Worldwide	0.89%	1.04%	1.18%	0.93%	1.44%	1.83%	27.8%

# FRAUD BY COUNTRY

As the chart below illustrates, the full-year fraud rates by country vary significantly. In developed markets, the fraud rates hover around 1.0% and most countries saw an increase in 2019 over the previous year's levels. In developing countries, such as Indonesia and Bangladesh, the fraud rates are often much higher.

Emerging markets can be a breeding ground for cybercrime given socioeconomic, infrastructure and other factors. By textbook definition, an emerging market is a nation that has the traits of a developed market but does not qualify to be called so because of lower standards of living. If online enterprises do not have proper controls in place, people can use the funds to plan terrorism, conduct fraud and launder money. Hence companies or financial institutions should be cautious and do proper ID verification before they offer any services. Strong KYC regulations and enforcement, in combination with cutting-edge identity verification technologies, could go a long ways in lowering new account fraud rates in these markets.

## FULL YEAR ID FRAUD RATES BY COUNTRY

Developed Markets	2014	2015	2016	2017	2018	2019	YoY Change
Italy	1.15%	1.07%	0.99%	0.82%	1.52%	1.35%	-11.24%
Spain	0.79%	0.66%	1.16%	1.24%	1.07%	1.16%	8.75%
Germany	0.86%	0.82%	0.82%	0.56%	0.62%	1.12%	80.73%
Canada	0.85%	0.77%	0.95%	0.60%	0.75%	1.08%	44.07%
France	0.80%	1.14%	1.10%	0.56%	0.70%	0.92%	30.51%
United States	0.53%	0.56%	0.65%	0.62%	0.66%	0.88%	33.65%
United Kingdom	0.96%	0.74%	0.73%	0.46%	0.70%	0.80%	13.81%

Emerging Markets	2014	2015	2016	2017	2018	2019	YoY Change
Indonesia	2.53%	8.95%	8.36%	8.25%	9.88%	11.14%	12.81%
Bangladesh	0.43%	1.99%	2.88%	10.02%	10.07%	4.69%	-53.41%
India	1.25%	3.01%	4.01%	3.46%	4.34%	3.91%	-9.89%
Nigeria	1.11%	1.39%	1.75%	1.95%	2.30%	2.72%	18.28%
Korea	1.25%	1.26%	1.26%	1.06%	0.78%	2.30%	196.26%
Russia	0.81%	1.02%	0.60%	0.73%	1.76%	1.76%	-0.19%
China	0.42%	0.50%	0.89%	0.65%	1.44%	1.24%	-14.16%
Philippines	0.70%	1.18%	1.51%	1.04%	1.06%	1.05%	-1.19%
Brazil	0.49%	0.91%	1.42%	1.11%	1.04%	1.35%	29.49%
Taiwan	1.38%	1.72%	1.78%	1.06%	0.84%	0.63%	-24.91%

# FRAUD BY INDUSTRY

New account fraud, where fraudsters open up new accounts under victims' names, increased to \$3.4 billion in the U.S. alone (source: Javelin Strategy & Research, 2019 Identity Fraud Study, March 2019). But the fraud rates vary significantly by industry as the table below suggests. While banking and other services have been hovering around 1% fraud, cryptocurrency and online gaming/gambling (which is largely an EMEA phenomena) witness significantly higher-than-average fraud rates.

Industry	2014	2015	2016	2017	2018	2019	YoY Change
Cryptocurrency	3.45%	2.75%	1.66%	0.66%	1.16%	3.23%	178.38%
Online Gaming	0.85%	1.13%	1.45%	2.30%	4.21%	2.52%	-40.21%
Financial Services	1.20%	1.81%	1.50%	1.20%	1.16%	2.10%	81.66%
Banking	n/a	1.55%	0.83%	0.63%	1.74%	1.53%	-11.80%
Services	0.94%	1.09%	1.28%	0.90%	0.98%	1.13%	15.44%
Retail	0.15%	0.46%	0.51%	0.59%	0.80%	1.04%	29.29%
Sharing Economy	n/a	2.03%	0.42%	0.52%	0.51%	0.57%	10.12%
Travel & Entertainment	0.12%	0.12%	0.20%	0.28%	0.34%	0.44%	28.38%
Totals	0.89%	1.04%	1.18%	0.93%	1.44%	1.83%	27.75%



## Cryptocurrency

Criminals use both old-fashioned and new-technology tactics to swindle their marks in schemes based on digital currencies. According to a [report by CipherTrace](#), \$4.26 billion has been stolen from cryptocurrency exchanges, investors and users in 2019 alone.

Presumably, the high rates of new account fraud, compared to banking, is because the industry is still not regulated. Cryptocurrency exchanges largely decide what kind of identity checks they will apply and they often place a higher premium on new account conversions, which means reducing extra security hurdles that will result in increased abandonment.

One of the consequences of having a lower KYC standard is that these exchanges are vulnerable to impersonation scams. Without proper identity verification in place, it's very easy for con artists to create bogus social media accounts and impersonate legitimate users. Cybercriminals may try to use these fake accounts to trick others via private or direct message into taking some kind of action in an attempt to defraud or compromise.





## Online Gaming and Gambling

New account fraud for online gaming and gambling has averaged 3% over the last three years.

In 2019, we witnessed new account fraud decline dramatically and we suspect that some of this decline is the result of the UK Gambling Commission's rules on when identity verification occurs. When a player opens an account with an online gambling site, the gaming operator needs to check who you are. It does this for three main reasons:

**1** to check you are old enough to gamble

**2** to check whether you have self-excluded from gambling

**3** to confirm your identity

Moreover, players must be verified 48 hours after account creation. Prior to this rule change, KYC checks could be performed after the player had gambled and verified when there was a cash payout.

Technological advancements in this industry have made online gambling more widely available and easier to access, which has attracted a growing number of first-time, unlikely players. This ever-growing industry has also attracted a new breed of fraudsters who are utilizing new account fraud to exploit the system, including:

- ✓ **Multiple Account Fraud**  
Fraudsters create dozens or hundreds of online accounts using fake credentials in order to tilt the balance in their favor.
- ✓ **Bonus Abuse**  
Whereby the numerous fake accounts benefit from new signup bonuses, coupons and other attractive offers.
- ✓ **Gnoming**  
The fraudster utilizes multiple accounts to help one player win. The other accounts lose deliberately so one can pocket all the wins and bonuses that go with it.

# PARTING WORDS

Many of the holiday fraud losses stem from fake accounts that are quietly and secretly created off-season, and then used during high-traffic days, where they can fly under the radar. This year's Holiday New Account Fraud Report highlights a number of important findings across regions, countries, industries and time.

Holiday fraud was down 13% from 2018 levels, but **28% HIGHER** on a full-year basis

Fraud levels in Asia-Pacific were **THREE TIMES GREATER** than the U.S.

Fraud levels in emerging markets, while varied, were **SIGNIFICANTLY HIGHER** than developed markets

The cryptocurrency and online gaming/gambling industries experienced higher-than-average fraud levels while the sharing economy and travel and entertainment industries experienced minimal fraud levels (i.e., less than 0.6%).

While the actual new account fraud during this year's holiday period was less than the full-year average, it was still 82% higher than 2014 levels. The real danger is that when fake accounts are created and not detected in time, they can be leveraged to make fraudulent transactions or exploited for money laundering.

Spotting fake accounts in a sea of legitimate users is difficult, but not impossible. Businesses often lack visibility into which accounts are used suspiciously until the fraud has already happened. Merchants often find out about the loss when a chargeback comes in from a credit card owner whose payment information was used in an illegitimate transaction.

As cybercriminals perfect and fine-tune their impersonation efforts, it is harder for online enterprises to distinguish high-risk from low-risk traffic. Too often, companies rely on traditional methods of identity verification which do not actually verify that someone is who they claim to be — they just verify the information that the user provides (name, Social Security number), all of which is available via the dark web or social engineering attacks.

Online identity verification can effectively lower fraud rates and deter would-be criminals by requiring a legitimate government-issued ID, paired with a corroborating selfie. This is why a growing number of online companies are turning to biometric-based identity verification and authentication technologies to definitively assess the digital identities of new and existing users.

Collectively, these technologies help weed out imposters and allow organizations of all types to protect their ecosystems against fraud.



## ABOUT JUMIO

When identity matters, trust Jumio. Jumio's mission is to make the internet a safer place by protecting the ecosystems of businesses through cutting-edge online identity verification and authentication services that quickly and accurately connect a person's online and real-world identities. Jumio's end-to-end identity verification solutions fight fraud, maintain compliance and onboard good customers faster.

Leveraging advanced technology including augmented intelligence, AI, biometrics, machine learning, certified 3D liveness detection and human review, Jumio helps organizations meet regulatory compliance including KYC, AML and GDPR and definitively establish the digital identity of their customers. Jumio has verified more than 200 million identities issued by over 200 countries and territories from real-time web and mobile transactions. Jumio's solutions are used by leading companies in the financial services, sharing economy, digital currency, retail, travel and online gaming sectors. Based in Palo Alto, Jumio operates globally with offices in North America, Latin America, Europe and Asia Pacific and has been the recipient of numerous awards for innovation. For more information, please visit [www.jumio.com](http://www.jumio.com).

**JUMIO**<sup>®</sup>