

# ONLINE MARKETPLACE

FRAUD TRENDS 2021



# CONTENTS

CHAPTER	PAGE	CHAPTER	PAGE
<b>1.0 Introduction</b>	3	<b>6.0 Growing fraud trends</b>	10
<b>2.0 What is an online marketplace?</b> Definitions	4	Fastest growing threats: promo, refund & supplier incentive abuse	
<b>3.0 The Covid-19 whirlwind</b> Marketplaces and the digital shift	5	<b>7.0 Graph networks</b>	18
<b>4.0 Fraud teams are growing</b> Merchants are investing in fraud budgets & team size	6	What are graph networks and why are they useful?	
<b>5.0 Top fraud risks</b> Your industry's top concerns: online payment fraud and ATO	9	<b>8.0 Machine learning</b>	20
		Marketplace use of machine learning & manual review	
		<b>9.0 Summary</b>	22



# 1.0 INTRODUCTION

Marketplaces, you experience fraud from all angles: customers and suppliers. On both sides, promotion and refund abuse are rising, and attacks are increasing from prolific fraudsters. Your business is a hot target, so managing all of these risks can feel like a tall order.

Do you have the right tools in place? Can you easily connect the dots? Are you aware of the hidden costs of emerging fraud?

This report will look at why fraud is rising against your business, with advice on how to prevent risks, reduce hidden costs and protect your customers.

## Survey methodology

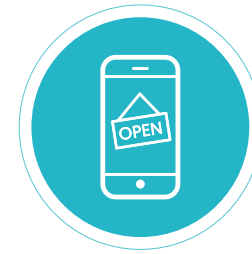
Ravelin surveyed over 1000 fraud professionals from countries around the world in 2020 - this report takes data from this **fraud & payments survey**. Survey participants work for online merchant businesses with over \$50million in annual revenue, in key ecommerce markets in Europe, Australia, North and South America. Survey participants are from a range of ecommerce industries under four main groups: Retail, Travel & Hospitality, Digital Goods and Marketplaces.





## 2.0 WHAT IS AN ONLINE MARKETPLACE?

Online marketplaces have many names (the sharing economy, third-party sellers, ride-hailing/ride-sharing) and it's confusing! Let's cut the jargon. Here are some simple definitions, including the three main marketplace types we'll look at...



### Online marketplace

An online platform that connects buyers with sellers, normally through an app. The platform is responsible for matching customers with vendors.



### Food

A platform where customers can choose from multiple restaurants or food vendors. The marketplace supplies and allocates a delivery driver.



### Taxi/cab/transport

A platform where customers can order a taxi and the marketplace will assign a driver to the job.



### Goods/services

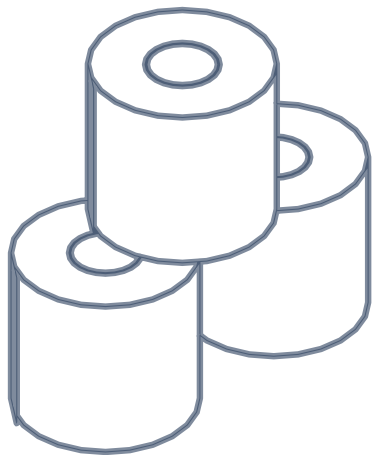
Customers can choose from multiple goods/services provided by third-party sellers on the platform.



## 3.0 COVID-19 THREW MARKETPLACES INTO A WHIRLWIND



We're 18 months into the Covid-19 pandemic and it's been a rollercoaster for ecommerce, but how did online marketplaces fare?



Food marketplaces boomed during lockdowns, as many customers **ordered food online for the first time** in 2020, looking for a stay-at-home treat. The appetite for food apps is still strong, as 85% say they will order delivery the same amount or more than they did pre-pandemic.

Goods marketplaces also soared, winning customers with options, convenience and reliability. With customers complaining of product shortages, (like **the Great Toilet Paper Shortage of 2020**) marketplaces gained an edge over traditional ecommerce retailers by filling supply gaps with agile delivery and multiple sellers.

But it wasn't good news for all marketplaces. Early 2020 Covid restrictions caused demand for taxi/cab apps to plummet - even leading app Uber reported a 75% decline in **bookings**. Thankfully, midway through 2021, demand for ride-sharing is **making a comeback**.

Overall, marketplaces hit all-time highs, taking **62% of all online retail sales** in 2020, growing at twice the overall ecommerce rate! But with great popularity comes great fraud risk. Here's how the digital shift is impacting fraud...



# 4.0 FRAUD TEAMS ARE GETTING BUSINESS-WIDE RECOGNITION

Has your fraud team gained appreciation since the start of the pandemic? We asked marketplaces the same question, and two-thirds said the perception of the fraud team had changed for the better.

### SURVEY PARTICIPANT JOB ROLES



Fraud / Payments Manager



Vice President or Director of Finance / Fraud / Risk



Fraud Analyst



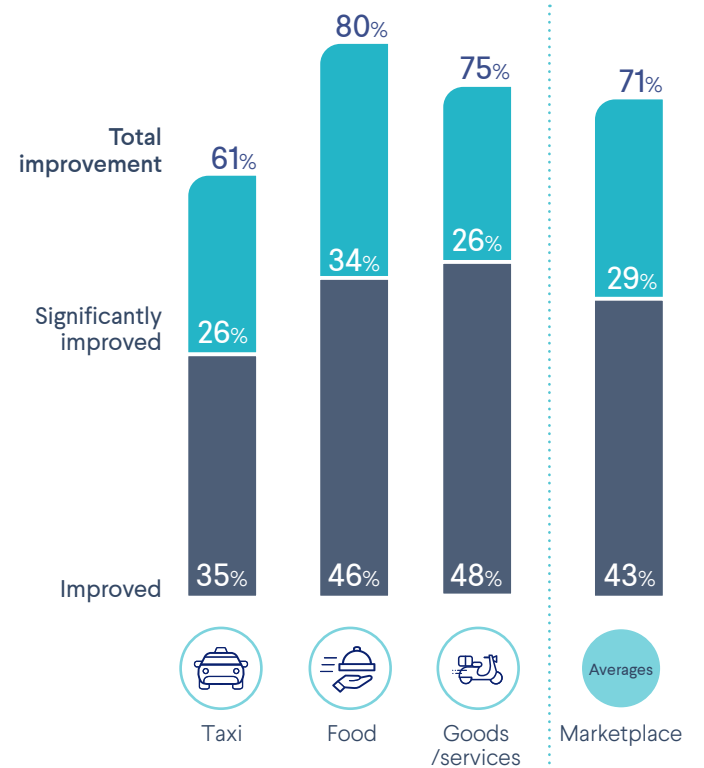
C Level:  
Chief Financial Office  
Chief Risk Officer  
Chief Technology Officer



# 71%

Marketplaces noticed an improvement in fraud team perception

### PERCEPTION OF FRAUD TEAM



On average, 71% of marketplaces noticed an improvement in fraud team perception, and just under a third of those said they saw a 'significant' change. The pandemic-led digital shift is making wider teams value security more than before.

Food marketplace fraud teams gained the most recognition, as around 80% saw perception improve. Over a third are noticing a 'significant' change. So here's one good thing to come out of the pandemic: fraud teams, you are getting some well-deserved appreciation!



# 4.1 MARKETPLACE PREDICTIONS OF FRAUD TEAM GROWTH

Are you expecting your fraud team to increase in size and budget? If so, then you agree with the rest of your industry...

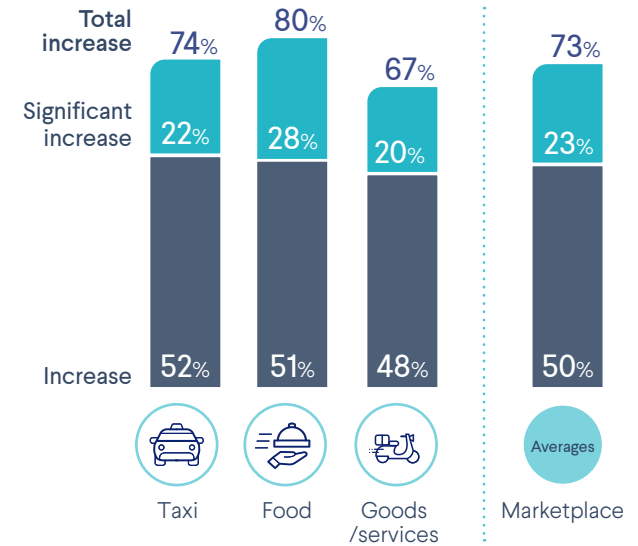


**73%** | Marketplaces are growing their fraud team

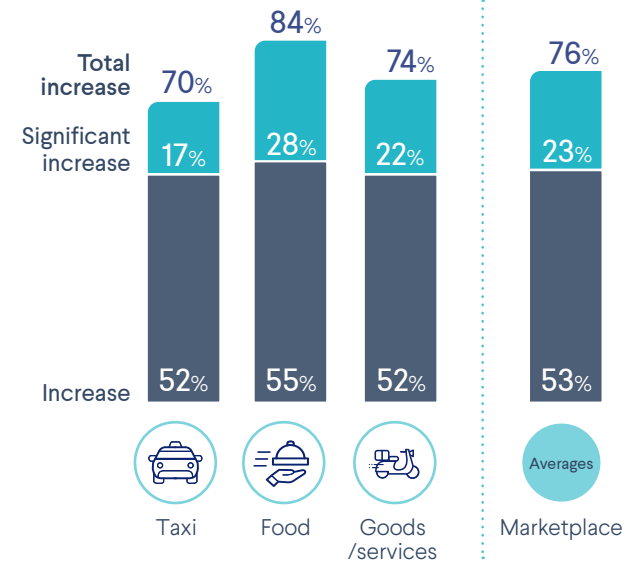


**76%** | Marketplaces are increasing the fraud budget

## SIZE OF FRAUD TEAM



## MARKETPLACE PREDICTIONS OF BUDGET GROWTH





Over three-quarters of marketplaces expect their fraud budget will increase, and 73% think the fraud team will grow. More marketplaces are expecting these investments than other industries, which is a huge pat on the back! Fraud is now grabbing the attention of C-level, as almost nine out of ten CFOs said their fraud budget will rise.

Marketplace fraud teams are getting more money and manpower, in line with their rapid growth amid the pandemic. Florian Jensen, Global Fraud & Payments Director at Glovo, explains that **investing in the fraud team** is the natural next step for fast-growing businesses:

“

As businesses grow, fraud will become more important. That 1% of fraud that might have cost a thousand Euros a month, is all of a sudden a million Euros.

**Florian Jensen**  
Global Fraud & Payments Director, Glovo



9/10

CFOs said their fraud budget will rise.

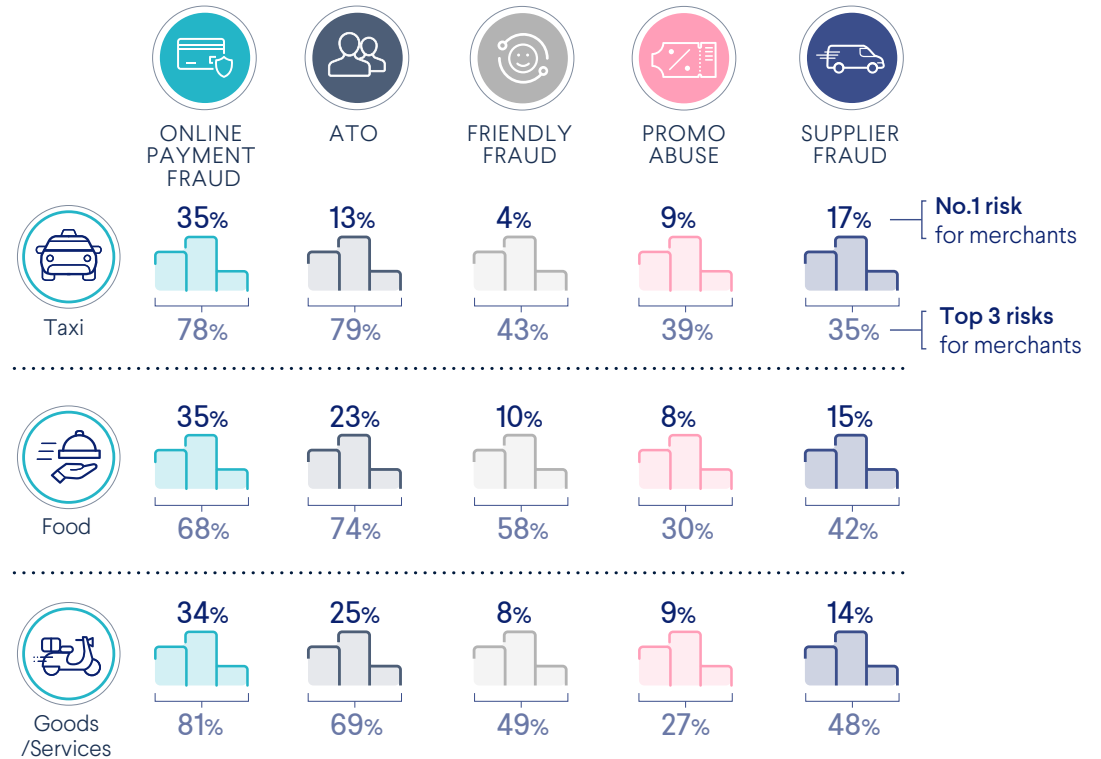




# 5.0 ONLINE PAYMENT FRAUD IS STILL CONSIDERED A TOP RISK

We asked marketplaces to rank fraud types according to the level of risk they pose to the business. Here's what you're most concerned about...

## TOP RISKS



Online payment fraud is still the number one concern of marketplace fraud teams, as over three quarters see it as a top risk, higher than any other fraud type. A whopping 81% of goods/services marketplaces ranked it top.

Account takeovers came in as the second biggest concern, as 71% put it in their top 3 on average. In fact, more food marketplaces put account takeover in their top 3 than online payment fraud.

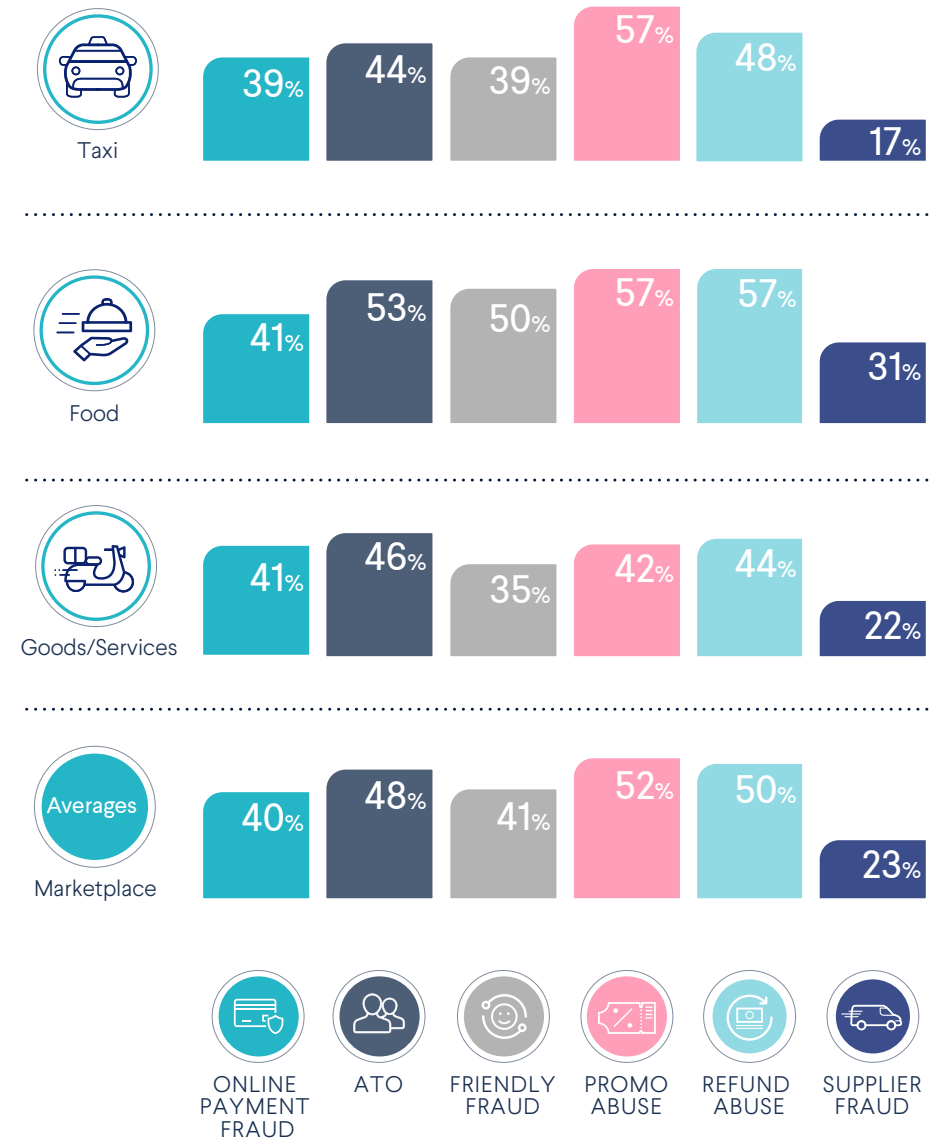
It's not surprising that more traditional fraud types ranked highly, as fraud teams will be more alert to well-known risks. But newer types of fraud are gaining momentum - while they may not be an obvious priority, they could be racking up hidden costs.



# 6.0 WHAT ARE YOUR FASTEST-GROWING FRAUD RISKS?

Would you have guessed that promotion abuse and refund abuse are rising faster than any other type of fraud?

PERCENTAGE OF MERCHANTS THAT ARE NOTICING AN INCREASE IN FRAUD ACTIVITY





# 6.1 PROMOTION ABUSE IS THE FASTEST-GROWING THREAT

Promotion abuse (promo abuse for short) is a type of online fraud that involves customers taking advantage of a business's offers. Whilst a few customers getting better discounts than they should doesn't sound too bad, it can leave businesses with eye-watering hidden costs.



# 52%

Marketplaces see promo abuse rise



**Promo abuse** is rising for over half of marketplaces. Taxi/cab and food verticals are seeing the biggest rise, affecting 57%, with almost a quarter noticing a significant increase. And that's just the merchants who are aware of it! Promo abuse often goes unseen.



**Marketplaces** are at risk of promo abuse as they are relatively young, so expansion is a priority and competition is tough. Every new app has to offer the best deals and easiest refunds.



**Covid-19** increased the risk of promo abuse, as more customers are looking for cheap rides or food so will push their luck with promos - if they can set up a few extra accounts and get 50% off their burgers more than once, they will!



**Taxi/cab marketplaces** saw one of the biggest rises in promo abuse, as ride-sharing apps upped incentives post-lockdown to convince customers to get back in cabs. Schemes like introducing free trips to and from vaccination centers hit headlines, tempting customers to take advantage.



**Food delivery** marketplaces also saw a huge rise in promo abuse, as increased demand intensified competition, and many had to offer more generous promotions to get an edge.



## WHY IS PROMO ABUSE A PROBLEM?



Do you know how much promotion abuse or refund abuse is costing your business? It's probably more than you think...

The costs of promo abuse are often hard to track, but since anyone with a smart device looking for savings can easily become a promotions fraudster, the numbers can quickly add up. Take Uber for example, one determined user racked up **£50,000 in future ride credits** by posting a referral code on Reddit – it can be an expensive issue.

Promo abuse can also damage brand identity and customer loyalty. If a customer's voucher is faulty, they'll spread the word. Or if your company makes it too easy to take advantage of promos, loyal customers could feel betrayed they're getting less for following the rules.

**New codes for Takeaway & Delivery**  
Straight to your inbox

Send Me New Codes

**GET FREE RIDES**  
Send friends a free ride and you'll get one too

SEND YOUR PROMO CODE  
**peterk6008ue**

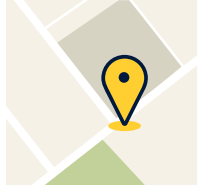
EMAIL INVITE

TEXT INVITE

Share on social media

**50% off**  
Monday to Friday

Use the Promo code



Green Station  
New York

SET PICK UP

Hail a ride with Gett, the best Taxi app  
**Download the app, get \$15\* with the code**  
\*for up to \$15 off your next rides

GTBORR



## 6.2 REFUND ABUSE HITS NEW HEIGHTS

Refund abuse (aka. returns abuse) occurs when a customer uses the returns policy of a merchant so much that it becomes unprofitable. Customers may also abuse refunds by faking returns/receipts, or reselling merchandise. Mainly carried out by genuine customers pushing their luck, refund abuse is not strictly considered to be fraud, but it is a problem.

Half of marketplaces noticed a rise in refund abuse in the past year, as the pandemic drove many to extend returns periods and offer contactless delivery. It became harder to track successful deliveries, so customers could easily say an order never arrived (even though it did).

A massive 57% of food marketplaces saw refund abuse increase - more than any other marketplace vertical. Refunds are so easy on food apps that customers can try their luck on every order - if they claim their food was cold when it wasn't, how can you prove it?



**50%** | Marketplaces see  
refund abuse rise



### WHY IS REFUND ABUSE A PROBLEM?

Refund abuse is difficult to stop. If you make return policies stricter, you might scare off customers - **83% of shoppers** will only buy from platforms with return policies they like. And if customers can't get a refund, they may file chargebacks, which can result in fines.

But if your refunds are too easy, refund abuse can get out of control - it's a difficult balance to strike. Marketplaces need to discourage serial refunding but keep good customers.



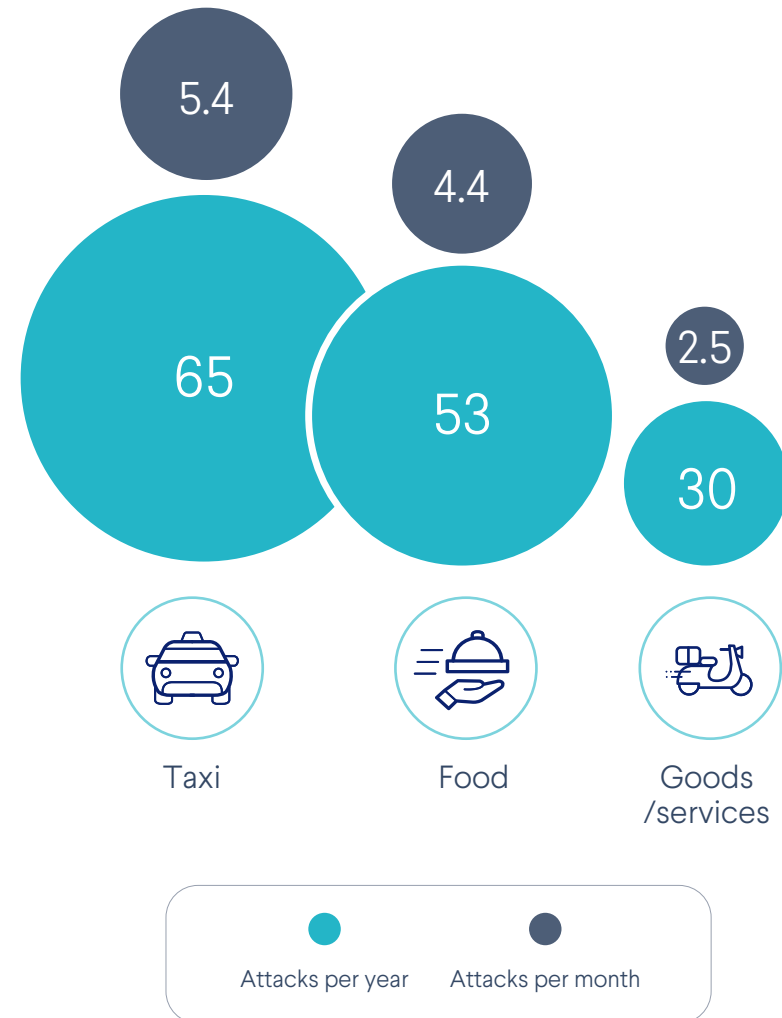
# 6.3 ACCOUNT HACKERS HEAVILY TARGET MARKETPLACES

Are you aware that Covid-19 increased the value of your customer accounts? Account takeover attackers are gaming the pandemic to their advantage, and marketplaces are at risk..



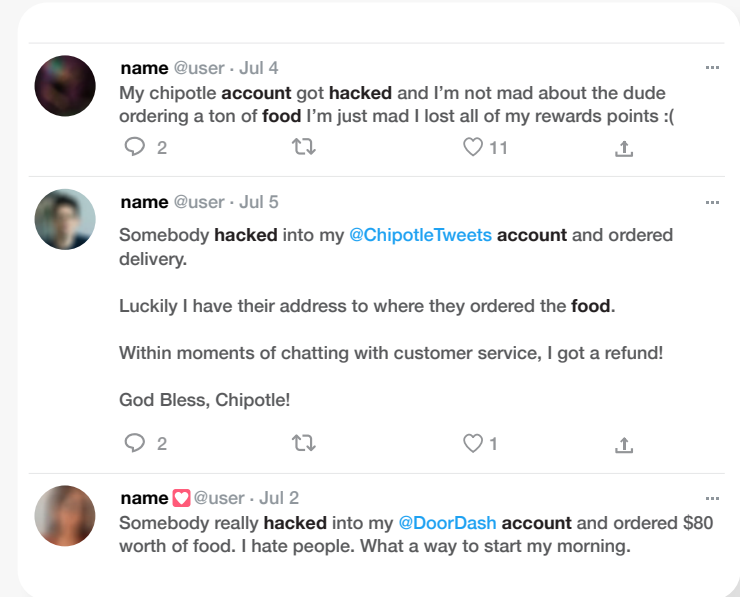
**Taxi/cabs see at least 1 account takeover attack per week!**

NUMBER OF ACCOUNT TAKEOVER ATTACKS IN THE PAST YEAR





Almost half of marketplaces are seeing account takeovers rise, as the pandemic ups the ante of attacks. Account takeover happens when a fraudster gets access to a genuine customer’s account, and since the start of the pandemic, there are a lot more accounts to hack.



**Marketplace** accounts may not seem like the most lucrative targets, but since they are in such high-demand, they are easy to resell.

**Taxi/cab marketplaces** are victim to more than one attack per week! In fact, they are the hottest target out of all industries. Attackers take over ride-sharing accounts and resell them for a profit. Since the pandemic, genuine customers might buy these cheap rides to avoid public transport. These accounts are also valuable to criminal groups so they can make dodgy journeys without being traced.

**Food delivery accounts** can be surprisingly lucrative to attackers. “Pizza plug” schemes are really popular and involve hackers taking over an account to resell food/drink at a discount. They can also order and resell items like expensive alcohol without the hassle of arranging delivery.

**Just Eat’s Fraud & Payments Manager, Shawn Colpitts**, explains that if you think you don’t have an account takeover problem, you probably just haven’t seen it yet...



If you haven’t discovered any account takeover attempts on your network, either your systems aren’t monitoring flags well enough, or your customer service procedures aren’t sending those indicators to the appropriate places.

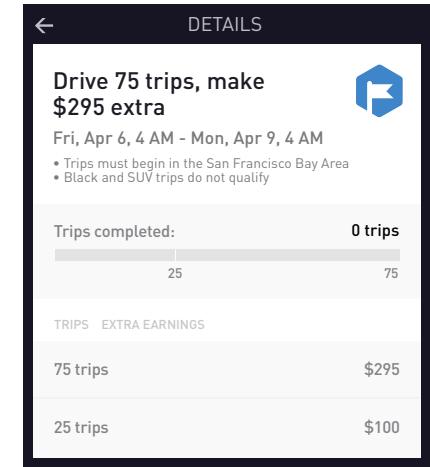
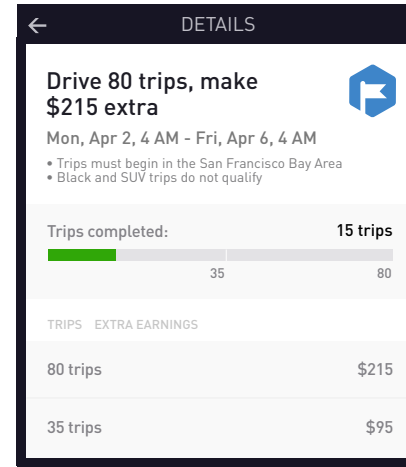
**Shawn Colpitts,**  
**Fraud & Payments Manager, Just Eat**





# 6.4 SUPPLIER FRAUD: A UNIQUE RISK WITH HIDDEN COSTS

Do you have a supplier fraud problem lurking under the surface? Marketplaces are at risk of fraud from their suppliers (vendors or couriers), and it can be costly and cause damage to brand reputation.



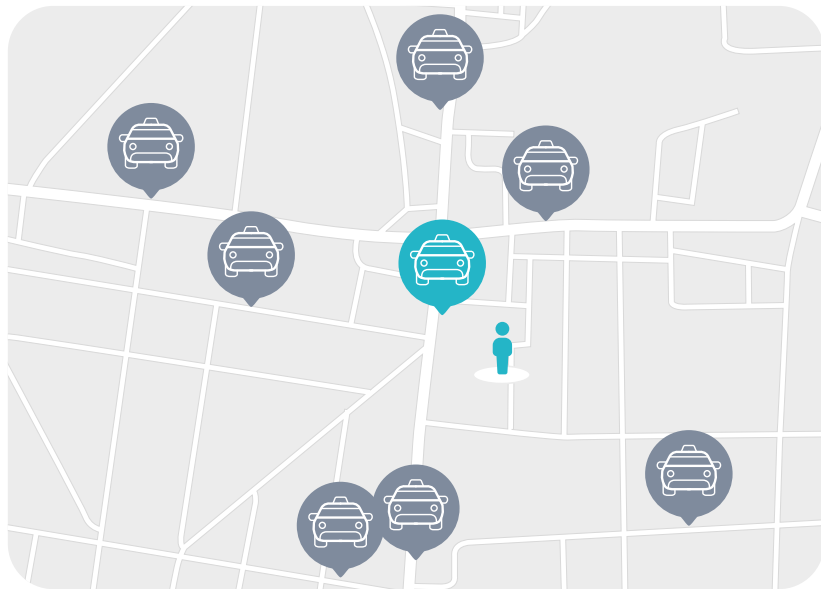
Supplier fraud mainly comes from **opportunistic suppliers abusing loopholes in incentive policies**. Cab drivers might run up the meter, or create fake accounts to order themselves and unlock a bonus. But sophisticated fraudsters can also enter your supply network and conduct organised crime operations like **money-laundering** or **modern slavery schemes**.





Just under a quarter of marketplaces noticed a rise in supplier fraud last year. On the surface this seems like it's growing less than other fraud, but it might be that businesses aren't really monitoring it or seeing the true scale. Customers are definitely noticing it increase, as titles like “customers accuse drivers of stealing their groceries” recently hit the press.

Taxi/cabs have become more vulnerable to fraud from their drivers since offering more **generous incentives to lure them back to work post-lockdowns**. Other marketplaces had to **round up enough drivers** to fulfil high order volumes. The more generous the incentive, the more lucrative it is for suppliers to try their luck.



## WHY IS MARKETPLACE SUPPLIER FRAUD A PROBLEM?

Supplier fraud is hard to identify and even harder to stop. If you haven't got the right tools in place, it can be disguised as genuine behavior and slip through the net.

**The main problem: you can't just block every supplier that might be behaving badly.** You need suppliers to grow and function. Plus, blocking just one could impact multiple customers, causing longer wait time, higher charges or other disappointment (like a cold meal).

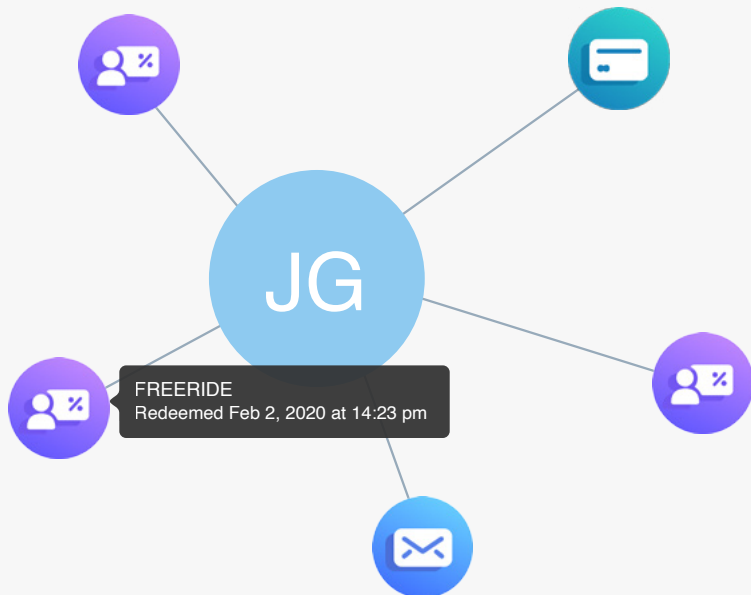
**It's not easy to measure your success at stopping supplier fraud.** Most scenarios won't result in a chargeback - a supplier wouldn't file a chargeback against themselves! Fraud teams often have to rely on anecdotal evidence, customer complaints, and manual review, which becomes less viable as your business grows.

**If you don't understand the connections between your suppliers and customers, you can never truly be in control of the situation.**

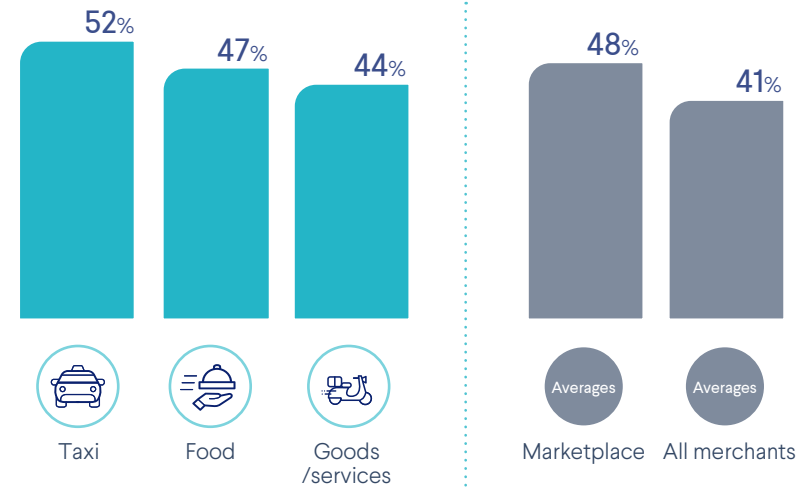


# 7.0 ARE YOU MISSING A TRICK WITHOUT GRAPH NETWORKS?

If you're one of the 52% of marketplaces not using graph networks to tackle fraud, you might be missing a trick...



PERCENTAGE OF MERCHANTS USING GRAPH NETWORKS



Graph networks are a key tool for managing marketplace fraud, making it easy to **evaluate connections between your data**. In a **graph network**, all the information about a customer's account, email, shipping address, order details and payment information is connected and visible at the same time. Marketplaces can also see their supplier data in the network, helping spot suspicious activity on both sides, giving you the bigger picture of your fraud.

It's good to see that marketplaces use graph networks more than other industries, and over half of taxi/cab merchants use them! Graph networks complement the immediate sales nature of marketplaces, as fraud teams can respond to risks in real-time without waiting for chargebacks.

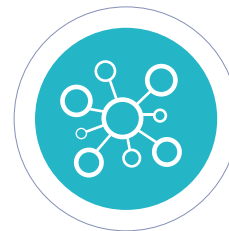
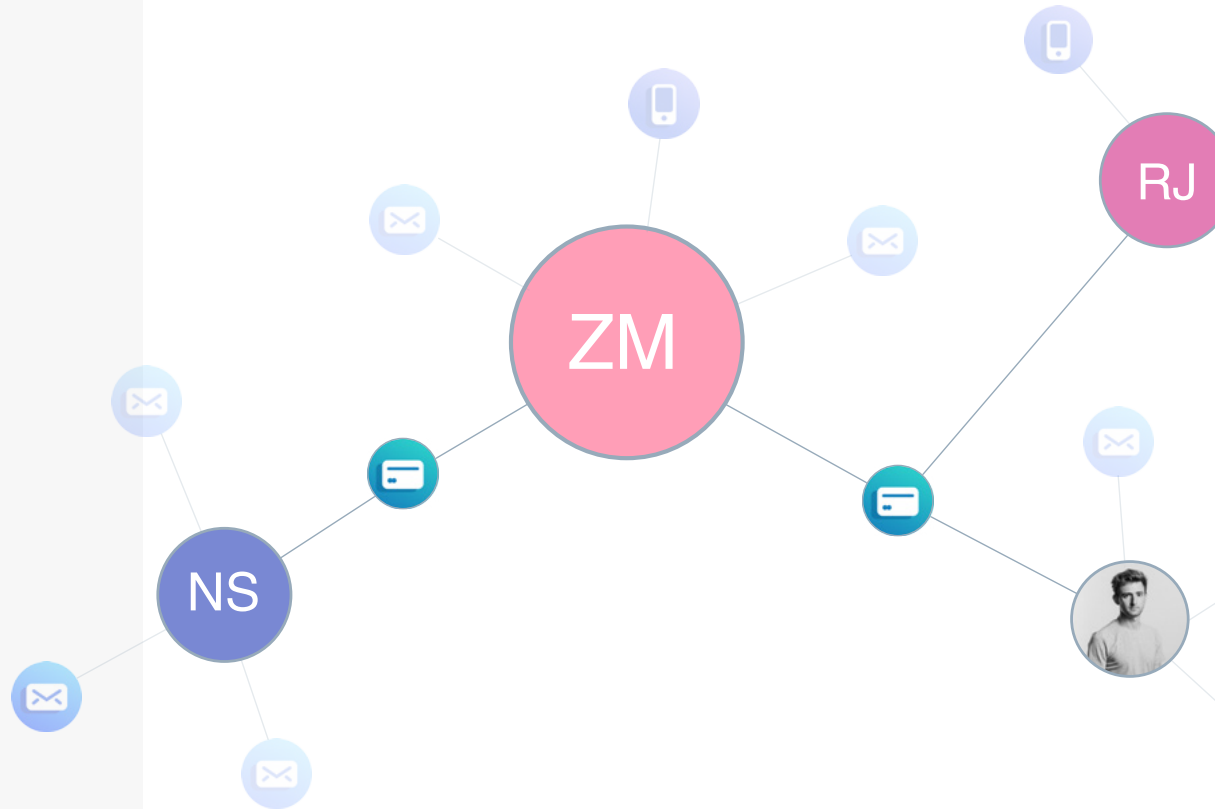


## WHY ARE GRAPH NETWORKS USEFUL?

Graph networks make suspicious connections and patterns clear - you can see your fraud visually, instead of just looking at data points. This works as fraudsters are often connected to others, as many exchange information/credentials on the dark web.

You can also look at suppliers in the network to spot connections between suppliers and customers. For example, if multiple customer accounts are connected by one supplier device, it's a good indicator of opportunistic behaviour.

Once you have all of the data in front of you, you can sort through grey areas and separate the policy abusers you want to keep, from the prolific fraudsters you should block.



**50%** | Marketplaces use graph networks



# 8.0 MARKETPLACES ARE FANS OF MACHINE LEARNING

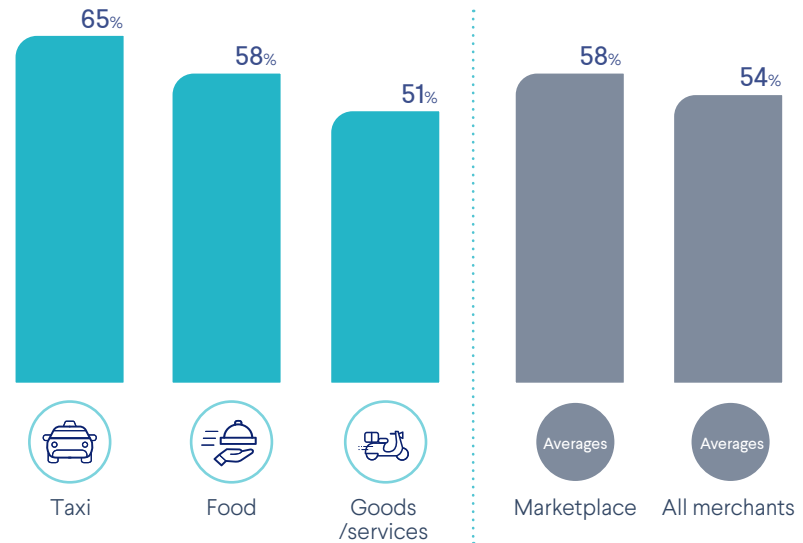
Did you know that marketplaces use machine learning more than other industries? On average, 58% are using this tool to prevent fraud, compared to 54% across other industries. This is because marketplaces are a new, digital industry, so are more likely to be up-to-date with the latest tech.



# 58%

Marketplaces use machine learning for fraud

PERCENTAGE OF MERCHANTS USING MACHINE LEARNING



Machine learning for fraud prevention involves training a model to recognise patterns and trends in your data to generate risk-based predictions. Machine learning is a bit tricky for marketplaces dealing with supplier fraud, as you can't simply label a driver as good or bad. Instead, you have to train a model to detect anomalies and make decisions after manual review.

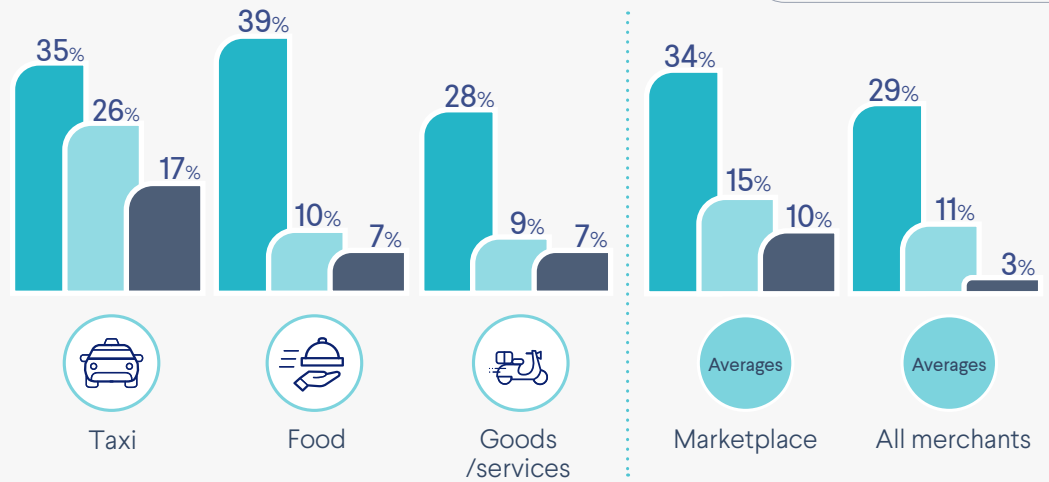
It's great that a huge 65% of taxi/cab marketplaces use machine learning, but teams need to stay agile amid the pandemic. If you don't keep your finger on the pulse, sudden changes and promos could appear suspicious to the model.



## WHY IS MACHINE LEARNING A USEFUL TOOL?

When used successfully, machine learning removes the heavy burden of data analysis from your fraud detection team. The results help the team with investigation, insights and reporting.

TIME SPENT ON MANUAL REVIEW



Machine learning doesn't replace the fraud analyst team, but gives them the ability to reduce the time spent on manual reviews and data analysis. This means analysts can focus on the most urgent cases and assess alerts faster with more accuracy, and also reduce the number of genuine customers declined.

This is important as marketplaces spend a lot of time on manual review. A quarter of your fraud teams spend the majority of time on it!

**For taxi/cab merchants, 43% of fraud teams spend 60%+ time on manual review.** If you think about supplier fraud, it makes sense that taxi/cabs would spend a lot of time on reviews, as the stakes are high if you wrongly block a driver - it could impact their livelihood.

No tool can replace the fraud analyst team, but you need to spend time efficiently and have the automated tools in place to cope, especially as your business grows. Machine learning and graph networks can take a lot of time pressure off.



**Ravelin's CEO, Martin Sweeney, explains:**

We can't overstate the vital role that humans play in fraud detection. The most effective fraud detection ecosystems comprise a combination of data and human insight and oversight because technology is only as good as the instructions it is given.

As your business grows, "automation is the only way to accurately and cost-effectively detect fraud among the sheer velocity and volume of online payments and account logins, and to detect abuse with refund requests and promotion use."



## 9.0 LOOKING FORWARD, WHAT CAN YOU EXPECT?

Marketplaces, prepare for a bumpy road ahead. The pandemic continues to create economic instability and uncertainty for ecommerce merchants across the world. **No one knows what's to come, but one thing's certain: fraud isn't going anywhere.**



Ravelin's CEO Martin Sweeney forecasts:

The recovery process is likely to be rocky and uneven. We've seen a dramatic shift in the retail market during the pandemic, with lockdowns moving merchants and customers alike online. This rise in e-commerce won't simply drop to pre-pandemic levels after Covid — it's very much here to stay — and online fraud is highly likely to stick around as well.”

Marketplaces will have to stay agile - you may have to adjust your approach to fraud in the face of unexpected new challenges.



## REPORT HIGHLIGHTS

### COVID-19 THREW MARKETPLACES INTO A WHIRLWIND

—  
Food and goods/services marketplaces saw record-breaking sales, but taxi/cab demand plummeted - all fraud teams continue to face unique challenges.

### MARKETPLACE FRAUD TEAMS ARE GETTING MORE RECOGNITION AND INVESTMENT

—  
Three-quarters of marketplaces expect their fraud budget and team will increase. The pandemic made teams realise the importance of fraud teams to online operations.

### ONLINE PAYMENT FRAUD AND ACCOUNT TAKEOVER ARE TOP RISKS

—  
Online payment fraud is the number 1 risk for over a third of marketplaces, and over 75% put it in their top 3. Account takeover is the second biggest concern.

### PROMOTION ABUSE IS THE FASTEST GROWING THREAT

—  
Promo abuse is increasing for 52% of marketplaces - a bigger increase than any other fraud type. Marketplaces are vulnerable as they tend to offer generous incentives.

### REFUND ABUSE HITS NEW HEIGHTS

—  
Refund abuse is rising for half of marketplaces, accelerated by contactless deliveries and generous returns periods.

### ACCOUNT TAKEOVER ATTACKERS ARE HEAVILY TARGETING MARKETPLACES

—  
Taxi/cab and food marketplaces were victim to one account takeover attack a week last year, and attacks are rising for 48% of marketplaces.

### SUPPLIER FRAUD CREATES HIDDEN COSTS

—  
Marketplaces are underestimating the risk of supplier fraud, and many don't have tools in place to get a grasp on the hidden costs.

### YOU'RE MISSING A TRICK WITHOUT GRAPH NETWORKS

—  
Not enough marketplaces use graph networks, as 52% don't have the tool. Without graph networks you can't easily see the full picture of your fraud.

### MARKETPLACES HAVE AN IMPRESSIVE ADOPTION OF MACHINE LEARNING

—  
Marketplaces embrace machine learning for fraud prevention as 58% use it. Marketplaces require a lot of manual review, so using the right automated tools is all-important.



# Thank you for reading the marketplace report

If you have any questions, feedback  
or comments please get in touch via  
the website.

.....

## GET IN TOUCH

Learn more about Ravelin's  
fraud and payments services at  
[ravelin.com](https://ravelin.com)