

TREMENDOUS



Fighting fraud in market research

Quirk's LA — February 2025

A client experienced

\$250,000

in fraud losses over a few months

Just a handful of fraudsters wreaked havoc




9 PayPal
accounts



10+ payouts
per account



\$40,000+ paid
to 1 fraudster



***“Fraud is turning into a large problem for us.
We’re handcuffed in our ability to deal with
the abuse.”***

Market research client

Today's presenter



Prateek Mehta

Product Manager

Tremendous

What we'll cover



How big of a problem is fraud for research firms?



How do fraudsters operate today?



What steps can you take to fight fraud effectively?

Research fraud is rampant today



Wherever you find payments, there are fraudsters

10%

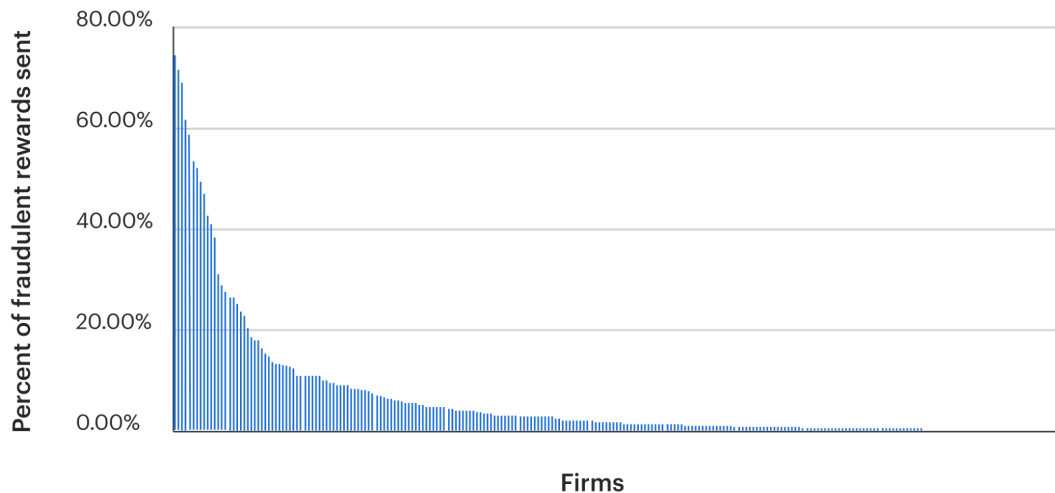
of research incentives go
to fraudulent participants

\$40k

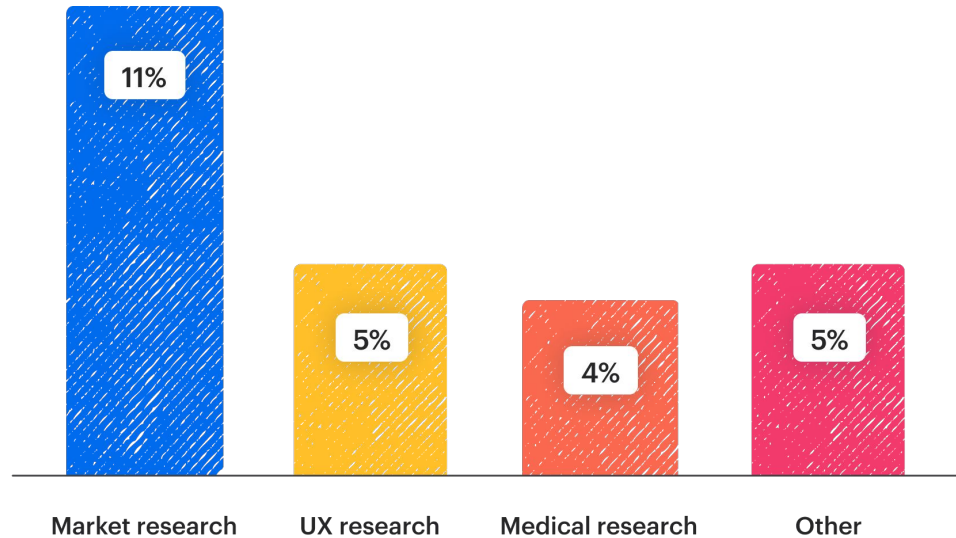
average lost by research
firms to fraud annually

**Fraud is
pervasive in
research**

Fraud rates per firm

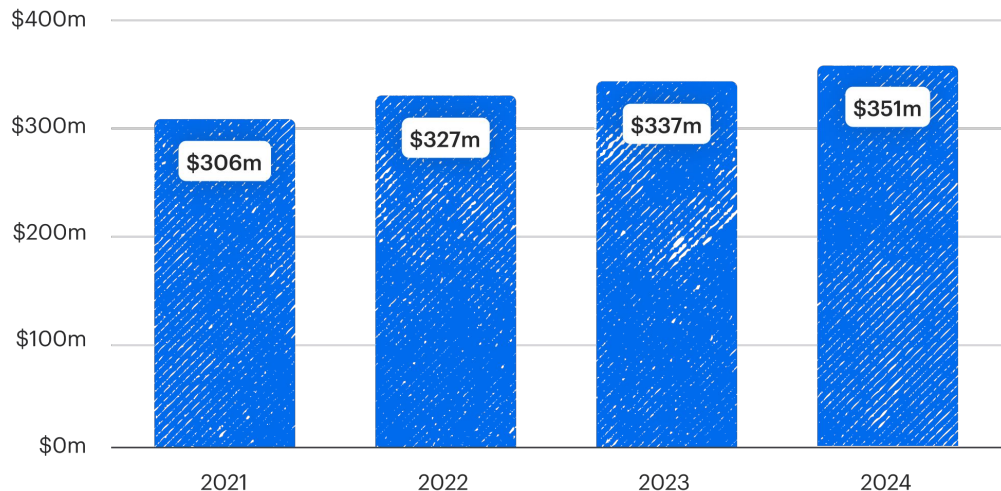


**Market
research is
most
impacted
by fraud**



**Market
research
firms lose
\$350M+
per year to
fraud**

Total fraud losses in MR industry by year



Profile of a fraudster



Common fraud methods used today



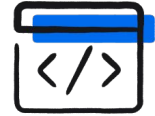
Phone
farms



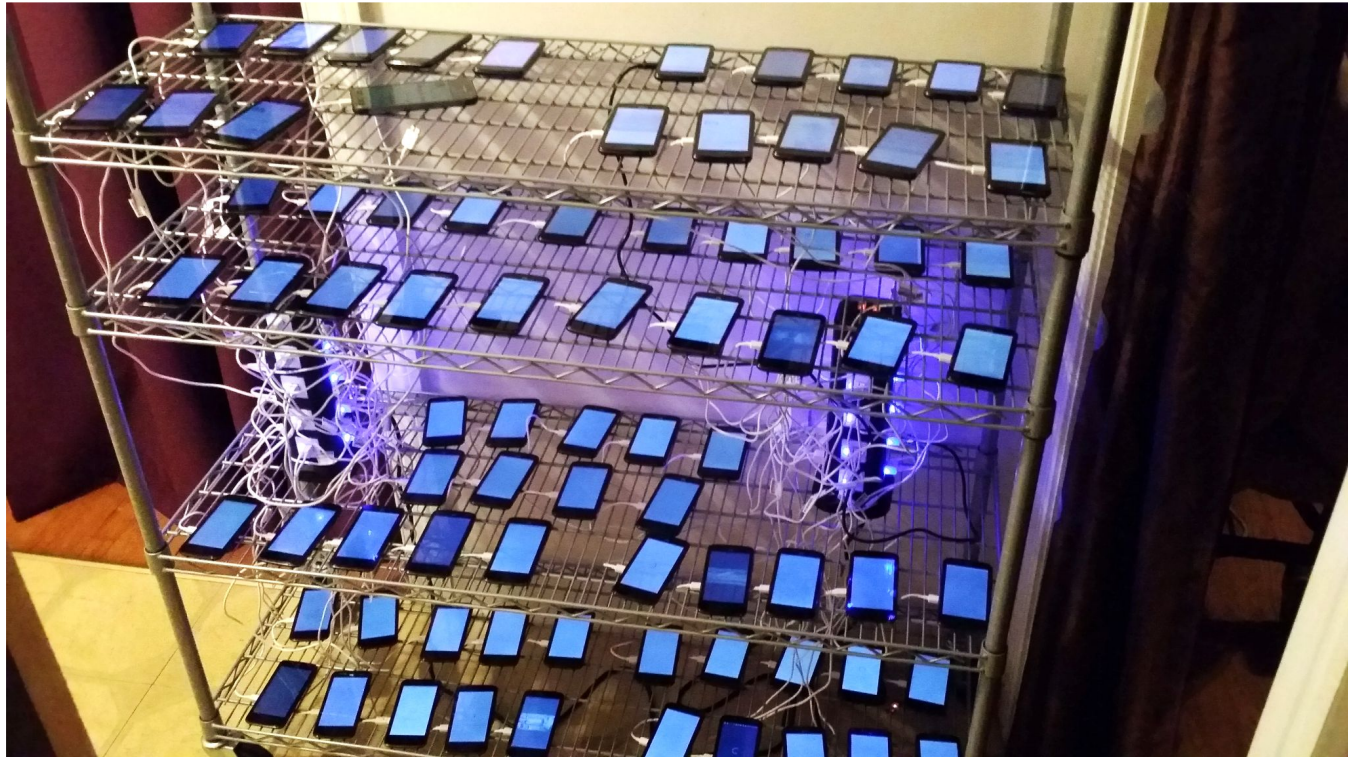
Multiple
emails



Multiple IPs /
VPNs



AI-generated
responses



Phone farm setup

Example fraudster profile










40 different emails

8 different IP addresses

3 different devices

Fraud trends by country

Instances of fraud by country

Country of IP address used at payout redemption	Percentage of fraudulent redemptions
 Nigeria	7.49%
 China	2.62%
 Bangladesh	2.53%
 Kenya	1.99%
 India	1.57%
 Tanzania	0.89%
 Saudi Arabia	0.86%

Fraudster hall of shame

2000+

emails created

700+

IPs generated

1100+

unique devices used

\$150k

in annualized "earnings"

27

companies defrauded

How to fight fraud effectively



Multi-layer approach to fighting fraud

1

Verify participants
prior to payouts
multiple times

Multi-layer approach to fighting fraud

1

Verify participants
prior to payouts
multiple times

2

Implement IP
identification and
risk scoring

Multi-layer approach to fighting fraud

1

Verify participants
prior to payouts
multiple times

2

Implement IP
identification and
risk scoring

3

Leverage your
network and share
data

Methods of scaling fraud prevention



Digital fingerprinting vendors



Fraud prevention algorithms



Fraud-focused internal hires



Payouts platform with built-in fraud prevention

How Tremendous fights fraud



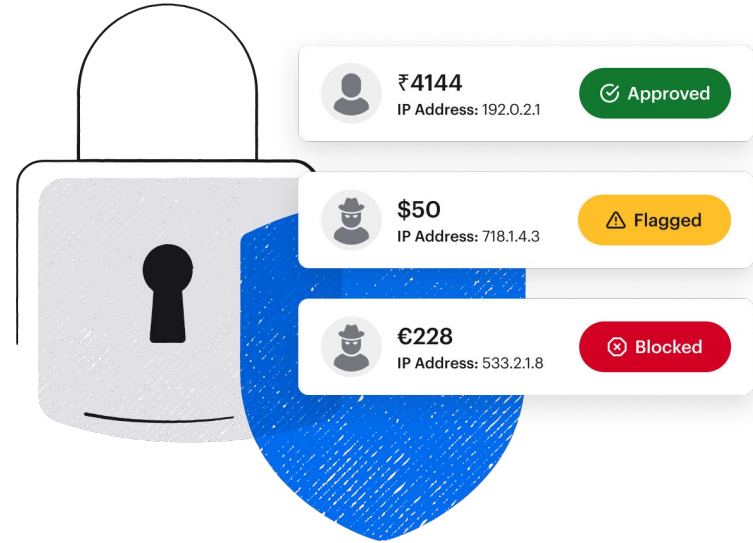
Since May 2024, we've detected over

\$3 million

in fraudulent payouts

With our fraud prevention tools, research firms can:

- Identify recipients cycling through identities
- Customize rules to detect fraud accurately
- Protect the experience for real participants



Fraud controls tailored to projects and participants

The screenshot displays the 'Fraud prevention settings' page within the Tremendous Parent dashboard. On the left, a dark sidebar contains a 'Menu' with options: Home, Fraud prevention (selected), Review queue, Settings (highlighted), Orders & rewards, Billing, Campaign templates, and Team settings. The main content area is titled 'Fraud prevention settings' with a 'Learn more' link. Below the title, the 'Review rules' section explains that reward redemptions matching any rule will be flagged. A list of seven rules follows, each with a 'Set up', 'Edit', or 'Disable' button. The rules are: 'Flag based on country' (Set up), 'Flag based on number of rewards redeemed' (checked, Edit), 'Flag based on dollar amount redeemed' (Set up), 'Flag specific IP addresses' (checked, Edit), 'Flag based on recipient email or domain' (Set up), 'Flag rewards redeemed by previously blocked recipients' (checked, Disable), and 'Flag based on the Tremendous fraud list' (checked, Disable). A final rule, 'Flag if device or account has multiple emails associated with it', has an 'Enable' button.

Team
Tremendous Parent

Menu

- Home
- Fraud prevention
- Review queue
- Settings
- Orders & rewards
- Billing
- Campaign templates
- Team settings

Fraud prevention settings

[Learn more](#)

Review rules

Reward redemptions that match any Review rules will be flagged and added to the Review queue

- Flag based on country** [Set up](#)
- Flag based on number of rewards redeemed** ✓ On [Edit](#)
Limit: 10 rewards / 30 days
- Flag based on dollar amount redeemed** [Set up](#)
- Flag specific IP addresses** ✓ On [Edit](#)
IP ranges: 0
Additional IPs: 1
- Flag based on recipient email or domain** [Set up](#)
- Flag rewards redeemed by previously blocked recipients** ✓ On [Disable](#)
Our system identifies recipients your team has previously blocked, even when they redeem from a different IP or email address, and flags any rewards they redeem for review.
- Flag based on the Tremendous fraud list** ✓ On [Disable](#)
Our algorithm detects suspicious recipients across millions of payouts within the Tremendous network and flags any rewards they redeem for review.
- Flag if device or account has multiple emails associated with it** [Enable](#)
Our system flags rewards redeemed by devices or accounts linked to multiple recipient emails.

Fighting fraud with the Tremendous network



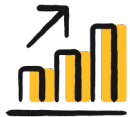
IPs / VPNs



Country



Email / domain



Transaction
volume



Total amount
redeemed



Blocked
recipients

Review and reconcile flagged transactions quickly

The screenshot displays the Tremendous user interface for reviewing fraud transactions. On the left is a dark sidebar with the Tremendous logo and navigation options: Team (Apple), Menu (Home, Fraud prevention, Review queue, Settings), and Orders & rewards (Orders & rewards, Billing, Campaign templates, Team settings). The main area is titled 'Fraud review queue' and includes a search bar and filters for 'Flagged' (1), 'Blocked', and 'Released'. A table lists a single reward with ID 'CVON...', amount '\$1.00', sent to 'pm@u.northwestern.edu', and status 'Flagged'. The reason for flagging is 'Over reward count limit, Over reward dollar limit'. On the right, a detailed view for transaction 'CVONKH5GRSTG' shows it is a \$1.00 USD flagged transaction. It includes buttons for 'Release' and 'Block', and a 'Recipient details' section indicating 'High risk' with reasons: '1 related reward (\$10.00), including 1 blocked', 'Over reward count limit', and 'Over reward dollar limit'. Further details include email, redemption card, device, and IP address.

TREMENDOUS

Team

Apple

Menu

Home

Fraud prevention Beta

Review queue 1

Settings

Orders & rewards

Billing

Campaign templates

Team settings

Search rewards, recipients, or orders

Fraud review queue

Flagged 1 Blocked Released

Search by reward ID, country, recipient email or phone

From: All time To: Today

Reward: 1

ID	Amount	Sent to	Status	Reasons
CVON...	\$1.00	pm@u.northwestern.edu	Flagged	Over reward count limit, Over reward dollar limit

CVONKH5GRSTG

\$1.00 USD • Flagged

Email reward sent to pm@u.northwestern.edu
Redemption attempted 2/5/24 at 14:00pm

Release Block

Recipient details

High risk

- 1 related reward (\$10.00), including 1 blocked
- Over reward count limit
- Over reward dollar limit

Email pm@u.northwestern.edu


Redemption merchant card

Device Cy0RmFIK0DEtFu1W79WG
1 related (1 blocked)

IP 160.72.66.134
New York, NY, USA
1 related (1 blocked)

Additional details

Activity log



“We've probably saved \$40,000 as a direct result of the fraud feature so far, both in incentives and study materials.”

Academic research customer

Audience Q&A



TREMENDOUS



Thank you

Stop by **Booth #617** to learn more