



MALVERTISING + AD QUALITY INDEX

# MAQ INDEX

---

CONFIANT'S MALVERTISING AND AD QUALITY (MAQ) INDEX (FORMERLY KNOWN AS THE DEMAND QUALITY REPORT) IS A QUARTERLY LOOK INTO CREATIVE QUALITY IN DIGITAL ADVERTISING. USING A SAMPLE OF OVER 150 BILLION IMPRESSIONS MONITORED IN REAL TIME EACH QUARTER, CONFIANT IS ABLE TO ANSWER FUNDAMENTAL QUESTIONS ABOUT THE STATE OF CREATIVE QUALITY.

---

**Q4 2021 | YEAR IN REVIEW**

MALVERTISING AND AD QUALITY REPORT





# INTRODUCTION

Confiant's **Malvertising and Ad Quality (MAQ) Index** (formerly known as the **Demand Quality Report**) is a quarterly look into creative quality in digital advertising. Using a sample of over 150 billion impressions monitored in real time each quarter, Confiant is able to answer fundamental questions about the state of creative quality.

Digital advertising delivers significant value to publishers but also introduces myriad risks related to security, privacy, and user experience. Malicious, disruptive, and annoying ads degrade user experience and drive adoption of ad blockers. However, few if any systematic studies have been conducted on the frequency and severity of ad quality issues as experienced by the real victims, end users.

Part of this is due to data issues: it had historically been challenging to estimate impact without client-side instrumentation in place on a large and diverse set of publishers. The advent of Confiant's real-time creative-verification solution in 2017 created a new way to examine the problem, revealing the underlying causes for the first time. The MAQ Index, which leverages Confiant's position as the vendor of choice for ad security, quality, and privacy monitoring, aims to provide a comprehensive view into the creative-quality issues facing the industry.

In 2018, Confiant released the industry's first benchmark report. This report, the fifteenth in the series, covers Q4 2021 and full year 2021.



# METHODOLOGY

To compile the research contained in this report, Confiant analyzed a normalized sample of more than 650 billion advertising impressions monitored from January 1 to December 31, 2021, from tens of thousands of premium websites and apps.

The data was captured by Confiant's **real-time creative verification solution**, which allows us to **measure ad security and quality on live impressions** (not sandbox scans) across devices and channels.

The violation rate is calculated by dividing the number of normalized impressions exhibiting a particular issue by the total number of impressions monitored by Confiant. Impressions for a particular issue type are normalized to reflect differences in activation rate among publishers.

All charts, with the exception of the per country breakout, are based on global data.



# MAQ INDEX 2022

## What's coming next

Confiant has published the **Malvertising and Ad Quality (MAQ) Index** on a quarterly basis since 2018. We have always considered it a labor of love and a contribution to the industry, as the report requires a significant resource commitment, most of which falls on a small team. These resource constraints have prevented us from delving as deeply as we'd like into the complex world of adtech to uncover the trends that merit being presented and reviewed by the industry.

We've therefore decided to shift to a twice-year publishing schedule for future reports. You'll still get everything you love about the MAQ Index — industry trends, SSP rankings, threat actor profiles — but we'll be able to supplement that with deep dives into new areas of interest. We'll also be able to track more SSPs and eventually include DSPs in the analysis.

We want to thank you, our loyal readers, for your interest and support over the past four years. We look forward to bringing you an even better MAQ Index in the future.



## SECURITY VIOLATIONS

Attempts to **compromise the user** through the use of malicious code, trickery, and other techniques.

Top issues include:

- **Malicious clickbait**
- **Forced redirects**
- **Criminal scams**
- **Fake ad servers**
- **Fake software updates**
- **High-Risk Ad Platforms (HRAPs)<sup>1</sup>**

## QUALITY VIOLATIONS

Non-security issues related to **ad behavior**, **technical characteristics**, or **content**.

Top issues include:

- **Heavy ads**
- **Misleading claims**
- **Video arbitrage (formerly In-Banner Video)**
- **Undesired audio**
- **Undesired video**
- **Undesired expansion**

---

<sup>1</sup> Ad platforms that consistently serve abnormal levels of malicious ads and are the preferred vector for malicious actors.





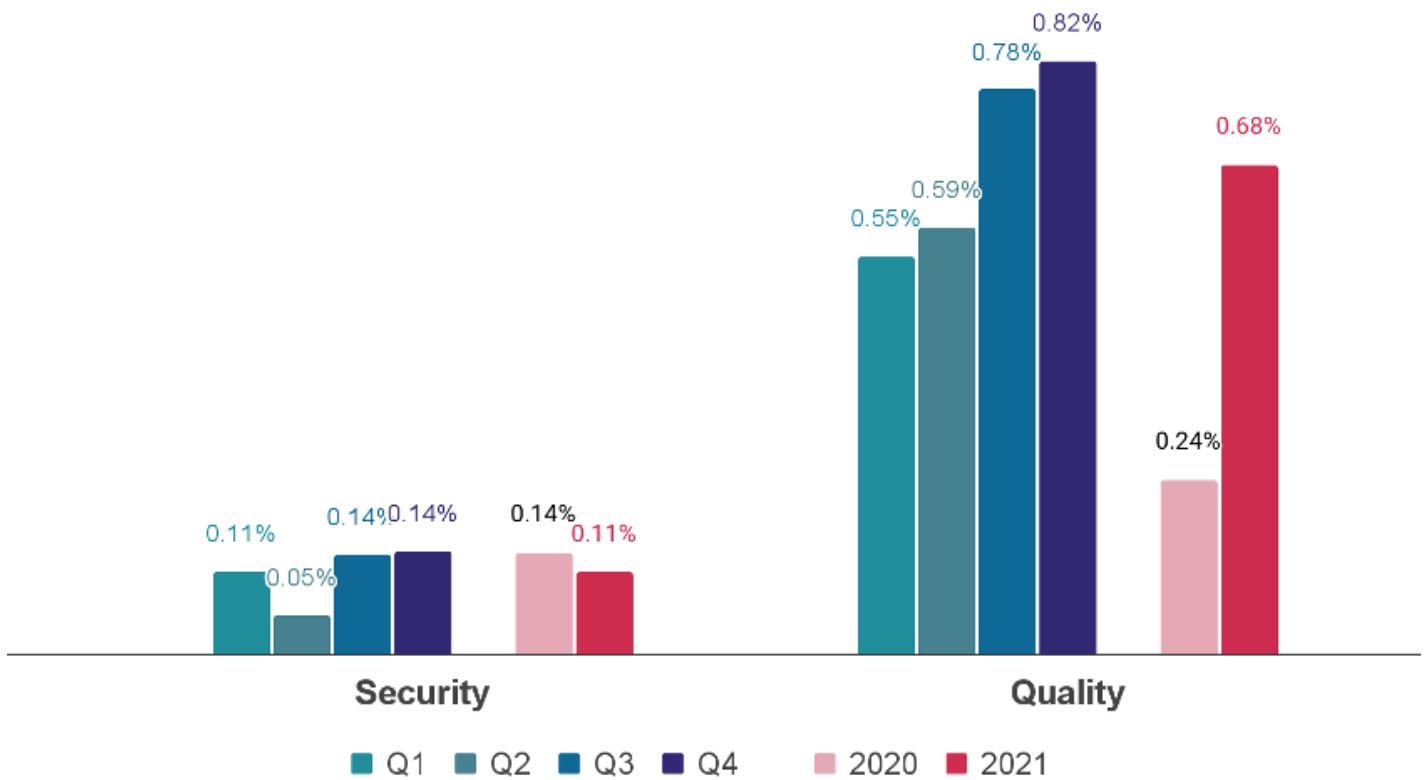
# INDUSTRY VIEW

---

**Q4 2021 | YEAR IN REVIEW**

MALVERTISING AND AD QUALITY REPORT



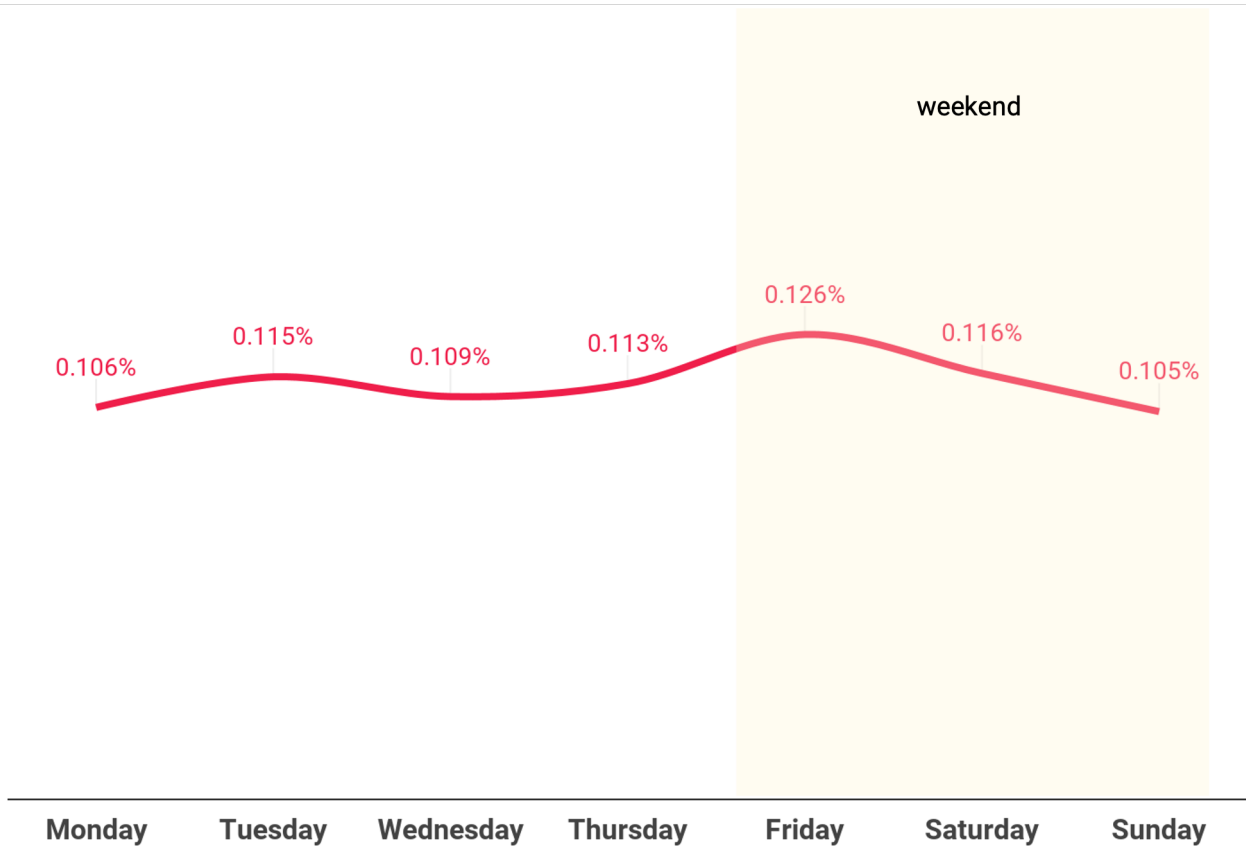


## How did the industry fare in 2021?



The **Security violation rate in Q4, at 0.14% of total impressions, matched Q3's high level**, which was already the highest in over a year. Looking at 2021 vs 2020, Security issues declined slightly to 0.11%.

The **Quality violation rate continued its steady rise, closing** the year out at 0.82%. **The rate of Quality issues has increased almost 50% from Q1 to Q4** and has increased for **six consecutive quarters**.



## Average Malvertising Rate by Day of Week in 2021

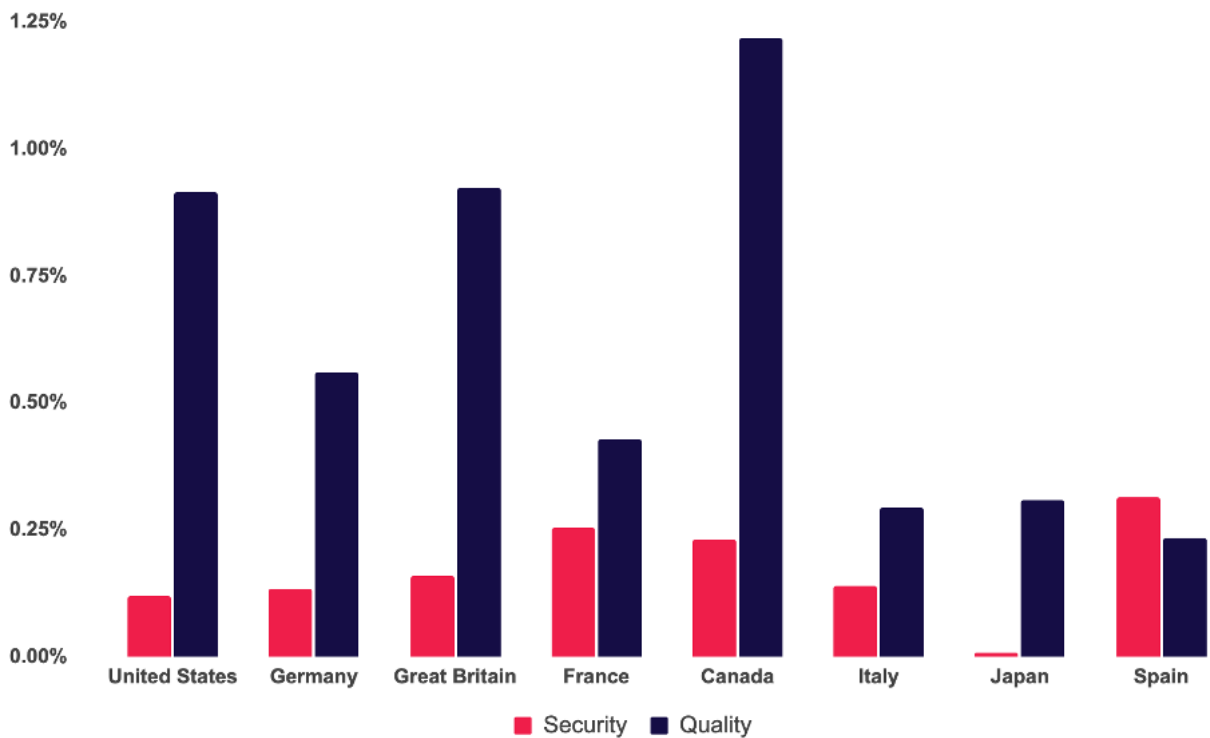


Conventional wisdom holds that malvertising activity picks up on the weekends as threat actors take advantage of lower staffing levels at publishers and platforms. But is that necessarily true? While in past years we did indeed see a marked increase in the rate of Security issues on the weekends, that disparity has declined over time. On average in 2021, Friday and Saturday were the days of the week with the highest violation rates, but the increase over the rest of the week was fairly modest.





In 2021,  
**1 in every 125**  
**ad impressions**  
was **dangerous** or  
**disruptive**  
**to users**



## Q4 2021 VIOLATION RATES BY COUNTRY

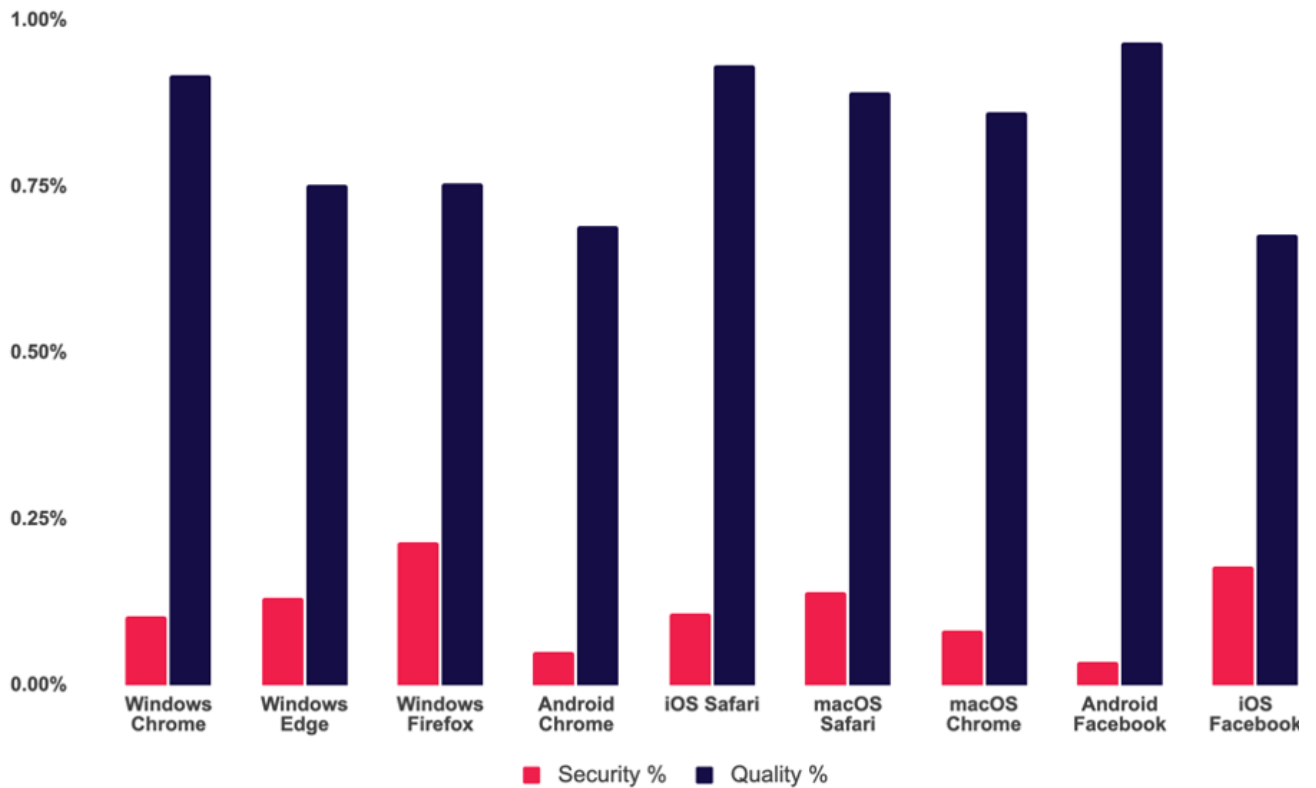


European markets remained more prone to Security issues in Q4, a pattern we've observed for some time. **In Great Britain, the Security violation rate more than doubled compared to Q3.** Conversely, the Security violation rate declined in Germany and Spain, but remained elevated.

Continuing a trend from Q3, **Quality violations were widespread in Canada, exceeding all other markets.** Japan's Quality violation rate more than tripled though remained low.





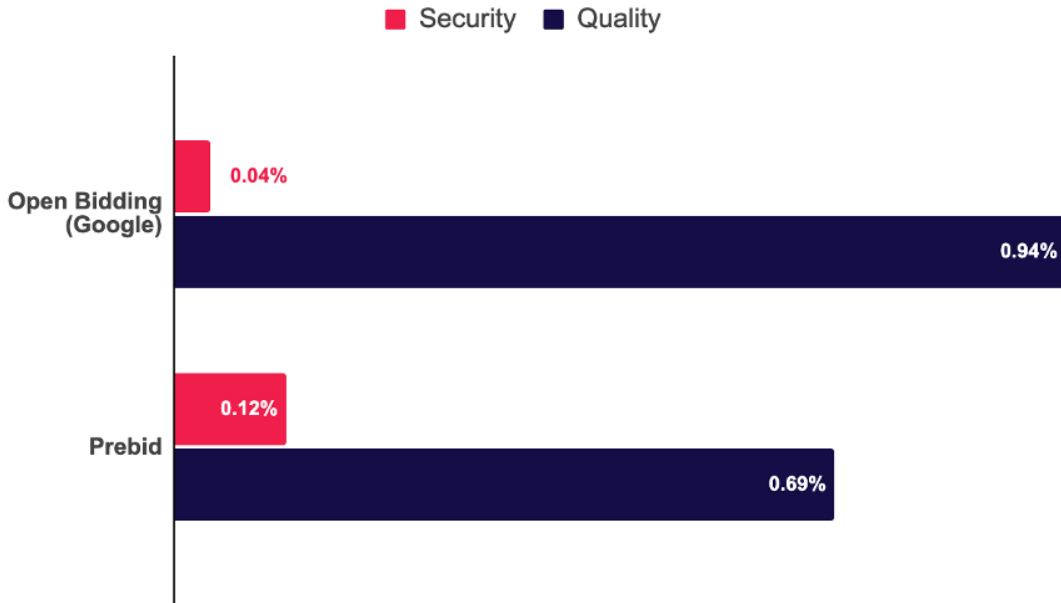


## Q4 2021 VIOLATION RATES BY BROWSER



**Firefox for Windows continued to be the worst performing desktop browser for Security issues**, a dubious honor it's held all year. On mobile devices, the browser integrated into **Facebook for iOS** repeated as the worst performer.

**Chrome had the lowest Security violation rates of all browsers** across all environments.

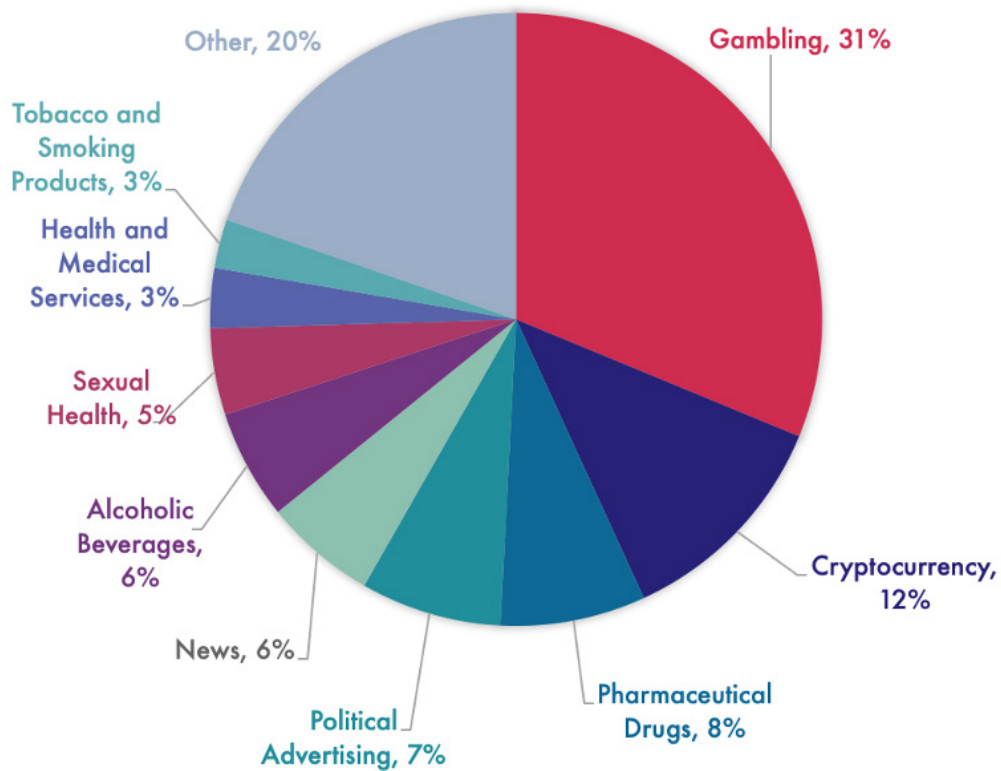


## Q4 2021 VIOLATION RATES BY HEADER BIDDING FRAMEWORK



Publishers use frameworks like **Prebid** to manage bidding from multiple SSPs. Google offers a similar feature within Ad Manager called **Open Bidding**. In both cases, demand from a diverse set of SSPs flows through the framework, putting the publisher at risk of Security and Quality issues.

**Google Open Bidding has consistently outperformed Prebid on Security issues**, and that dynamic remained true in Q4. Conversely, Prebid performed better than Open Bidding on Quality issues for the second quarter in a row.



"Other" includes over 100 other categories

## MOST BLOCKED AD CATEGORIES



Confiant allows publishers to block creatives across 100+ different categories, including common verticals like Automotive and sensitive topics like Alcoholic Beverages.

In Q4, **Gambling remained the most blocked ad category**, a position it has held for three straight quarters. Reflecting the rise of web3 offers and scams, **Cryptocurrency joined the field this quarter, taking 2nd place. Pharmaceutical Drugs** followed at 3rd.

**Political ads returned with a vengeance** in the Q4 election season in the U.S., taking the 4th spot.





In Q4,  
**Confiant blocked  
nearly 200million  
Gambling ads**





# SSP RANKINGS

---

**Q4 2021 | YEAR IN REVIEW**

MALVERTISING AND AD QUALITY REPORT





## Q4 2021 US SSP Rankings

In Q4, Confiant tracked impressions from over **100 SSPs**. However, the vast majority of **global impressions originated from just 12 providers**<sup>1</sup> commonly used by publishers. These 12 providers are noted in the charts that follow using a coding system that carries over from one quarter to the next to allow comparisons over time.

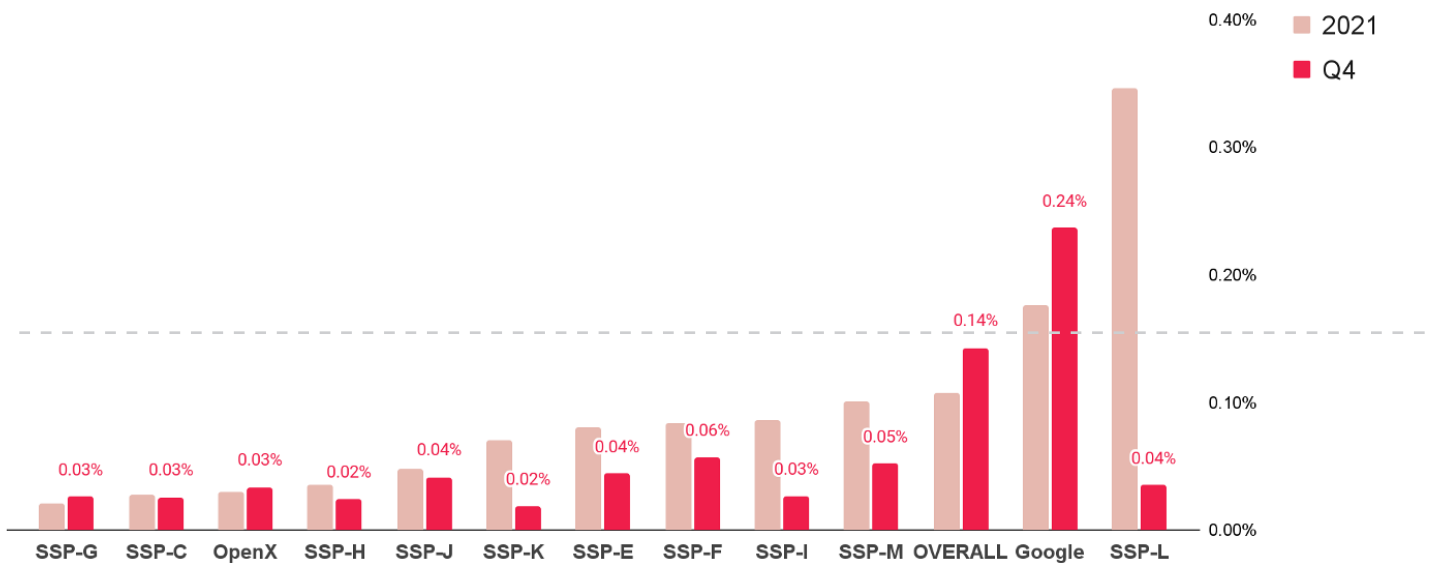
To qualify for inclusion, a provider had to have been a consistent source of **at least 1 billion Confiant-monitored impressions** a quarter across our global sample.

We identify two SSPs in these rankings: **Google** and **OpenX**. As the operator of the largest exchange, Google has access to data and resources beyond what's available to other exchanges. **OpenX** has opted to be listed in our reports **without obfuscation, an option we offer to any SSP that requests it**. We encourage other leading SSPs to request full disclosure so that we may provide the publisher community with a complete view into relative quality of their partners.

---

<sup>1</sup> Google, Magnite, OpenX, Xandr, Yahoo, Index Exchange, PubMatic, Sonobi, TripleLift, Sharethrough/DistrictM, 33Across, and Sovrn





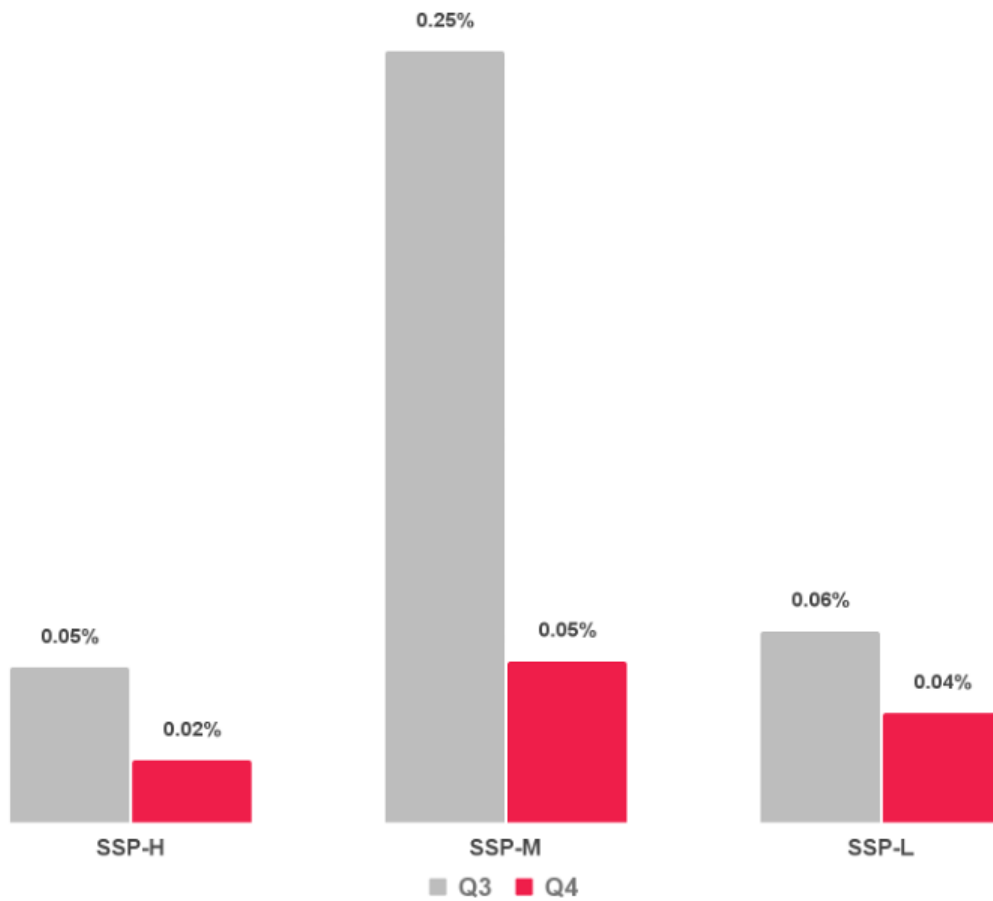
## Q4 AND 2021 SECURITY VIOLATION RATE BY SSP



For most SSPs, Security violation rates in Q4 largely tracked their performance for the full year. Exceptions included **SSPs K, L and I, which showed significant improvement** in Q4 vs the rest of 2021. **Google** remained an outlier in terms of both security violation rate and type, with Q4 exceeding their overall 2021 violation rate, Google’s issues here are being driven by **fake download ads**, not malware, for which more information is provided on slides 25 and 30.

**SSP-L showed the biggest improvement** after struggling early in the year. They turned things around in Q3, and their violation rate in Q4 was a mere 0.04%.

The top performers for the year for Security were **SSP-G**, **SSP-C**, and **OpenX**.

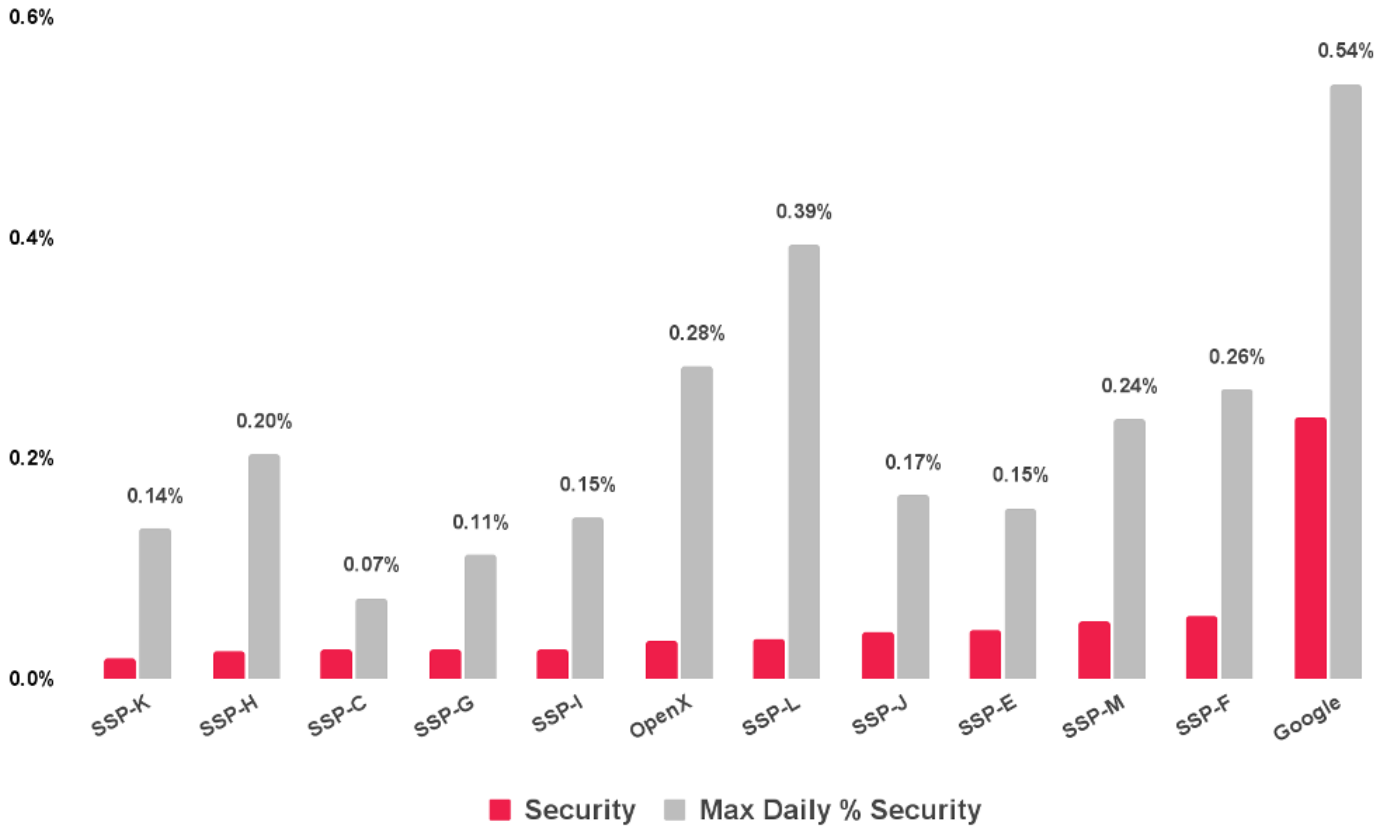


## SECURITY VIOLATION RATE: Q3 VS. Q4



**SSPs M, H, and L dramatically reduced their Security violation rates from Q3**, making them the Q4's most improved SSPs.

**SSP-L in particular has shown tremendous progress** over the course of 2021, ending the year with a violation rate well below the industry rate.

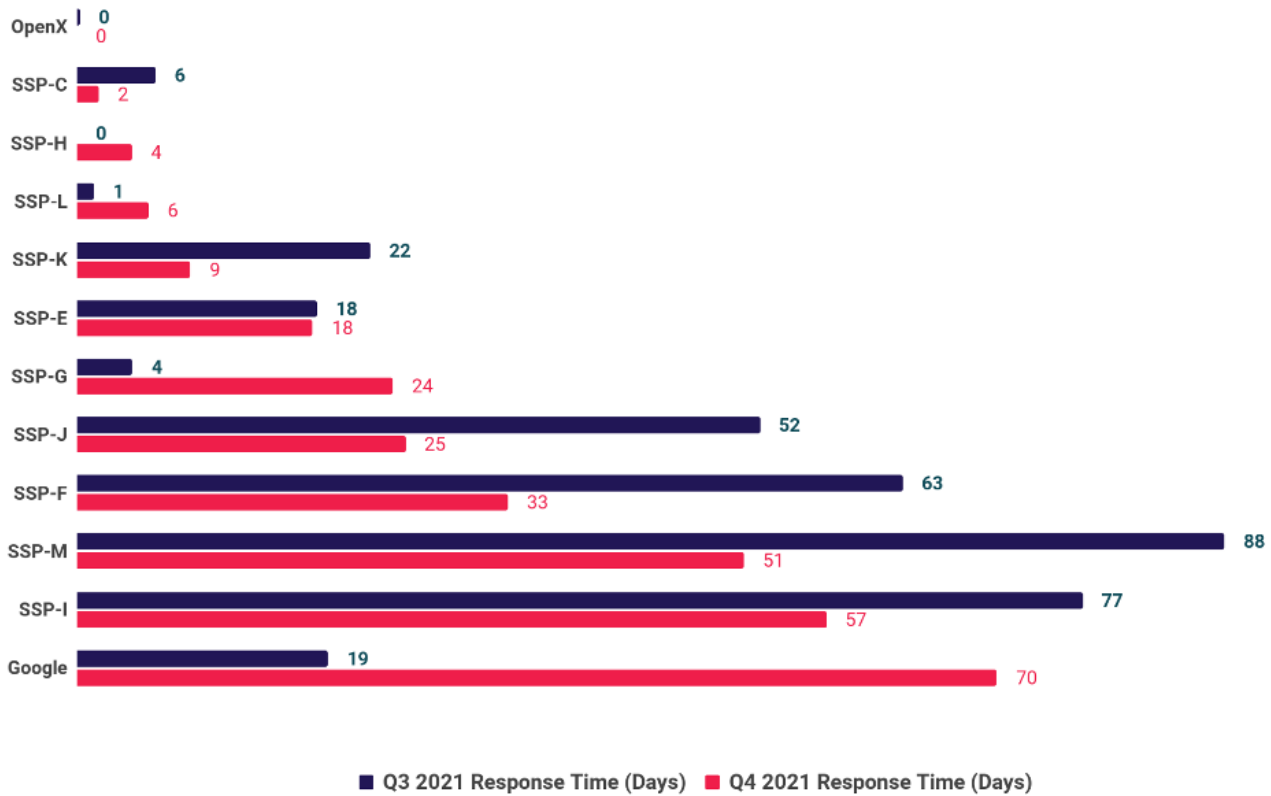


## Q4 DAILY MAXIMUM SECURITY RATE BY SSP



Quarterly averages can mask significant variation in day-to-day performance, so it's important to note the **upper bound of the Security violation rate** for each SSP to get a sense of overall risk.

In Q4, **Google recorded the highest daily security rate for the quarter**, at 0.54%, though this was less overall variance to its base rate than other SSPs (2.1x for Google vs. 5x to 10x for others). Other outliers included SSP-L, at 0.39%, and SSP-E, at 0.31%



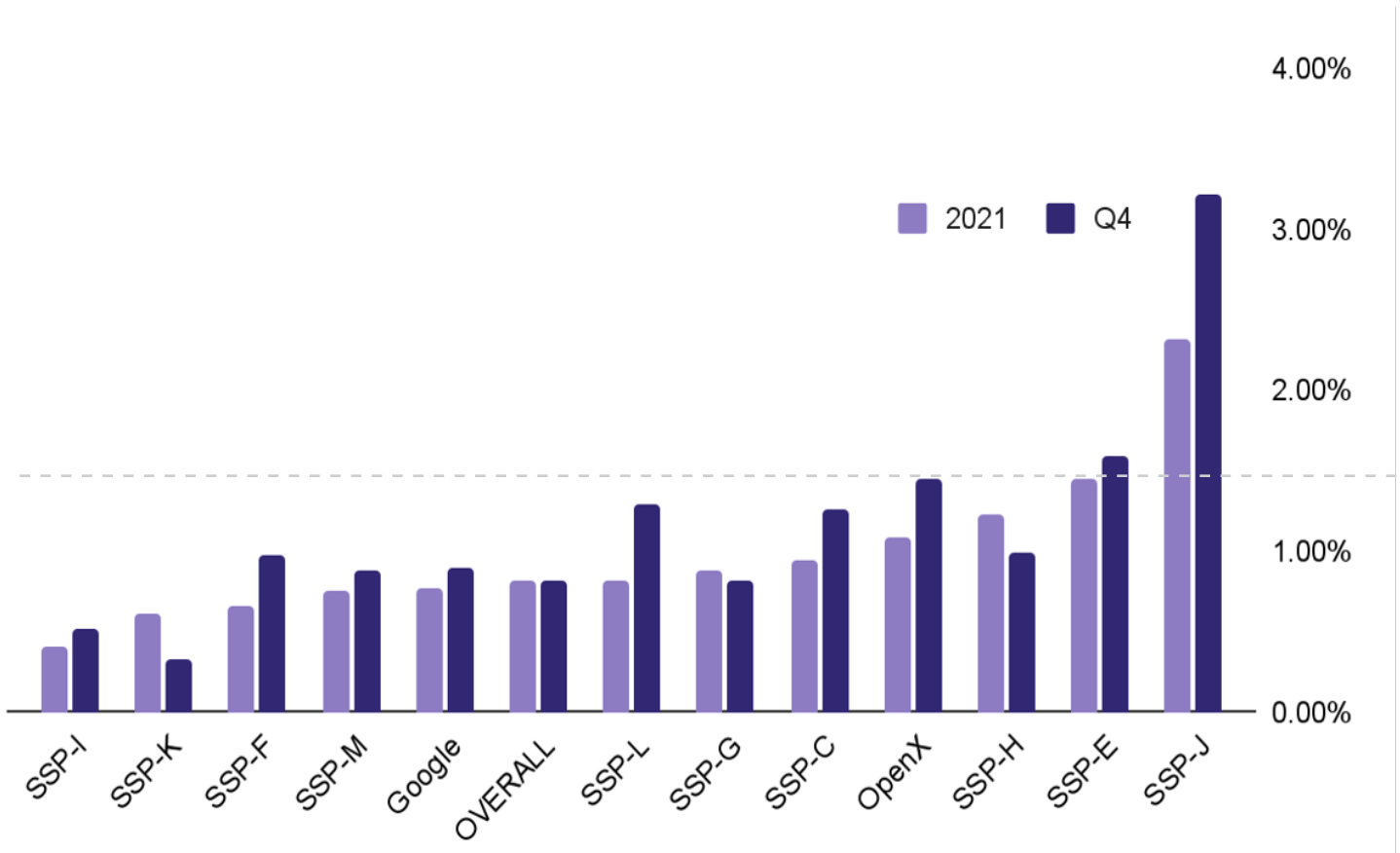
## AVG DURATION OF ATTACK BY SSP Q3 OVER Q4



SSPs differ in their ability to respond to attacks once they are underway. We measure how long it takes from when a threat first appears on an SSP to when it's last seen. On this measure, we see huge differences among the major SSPs.

In Q4, **OpenX's average response time remained below 1 day**, an extremely strong performance.



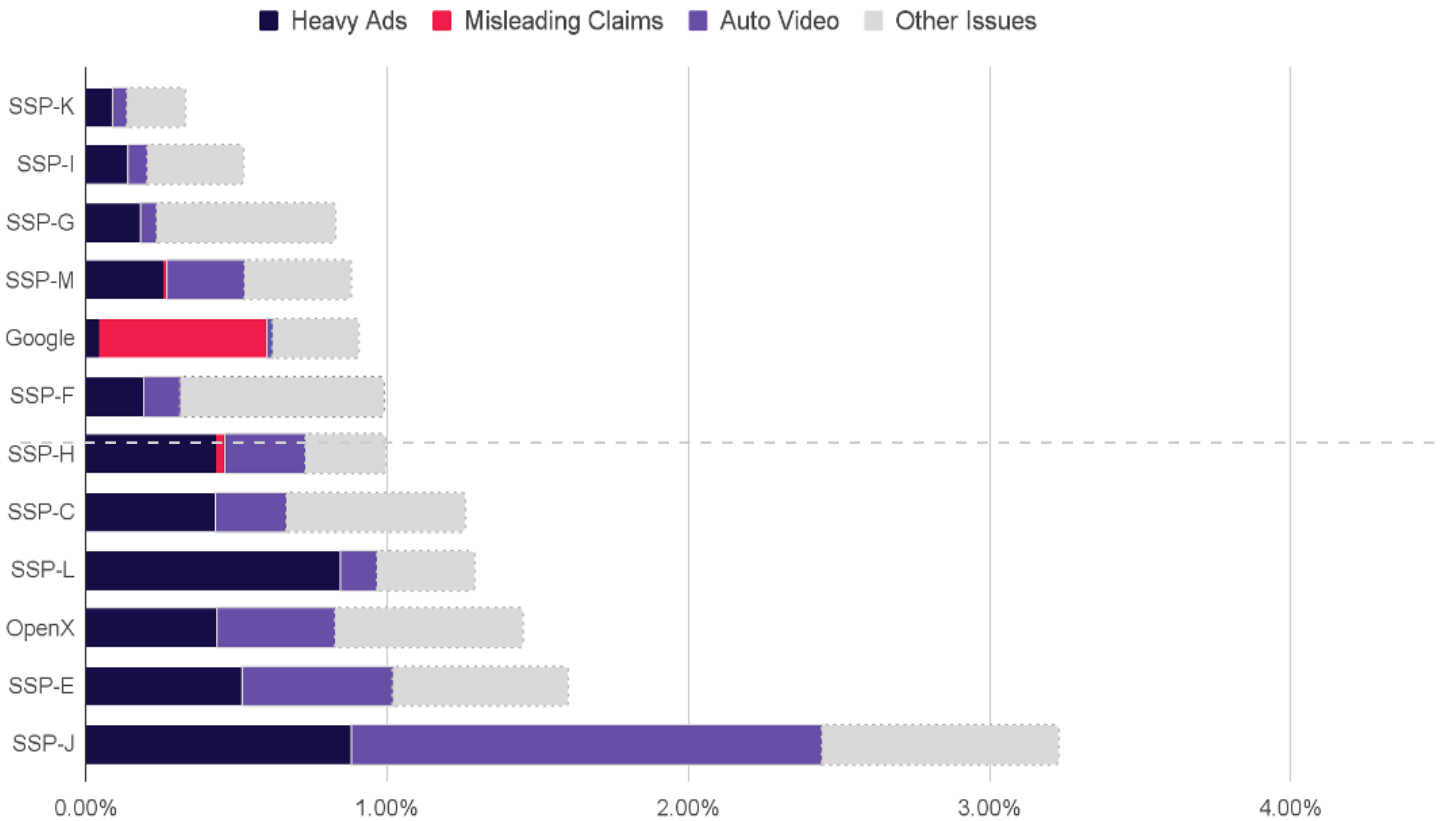


## Q4 AND 2021 QUALITY VIOLATION RATE BY SSP



**Quality violations** are based on a diverse set of controls that publishers can activate on the Confiant platform. Examples include **Auto Video, Heavy Ads,** and **Misleading Claims.** These controls correspond to ad behaviors that disrupt or impair the user experience.

A consistently poor performer on Quality issues, **SSP-J trailed all other major SSPs in both Q4 and 2021.** Conversely, **SSP-I has consistently been among the best performers for Quality.**



## QUALITY VIOLATION DETAIL FOR Q4



For most SSPs, **Heavy Ads** (ads where the total network load exceeds a KB threshold set by a Confiant publisher) and **Auto Video** (ads that play video immediately after rendering without any user interaction) tended to be the most prominent Quality issues.

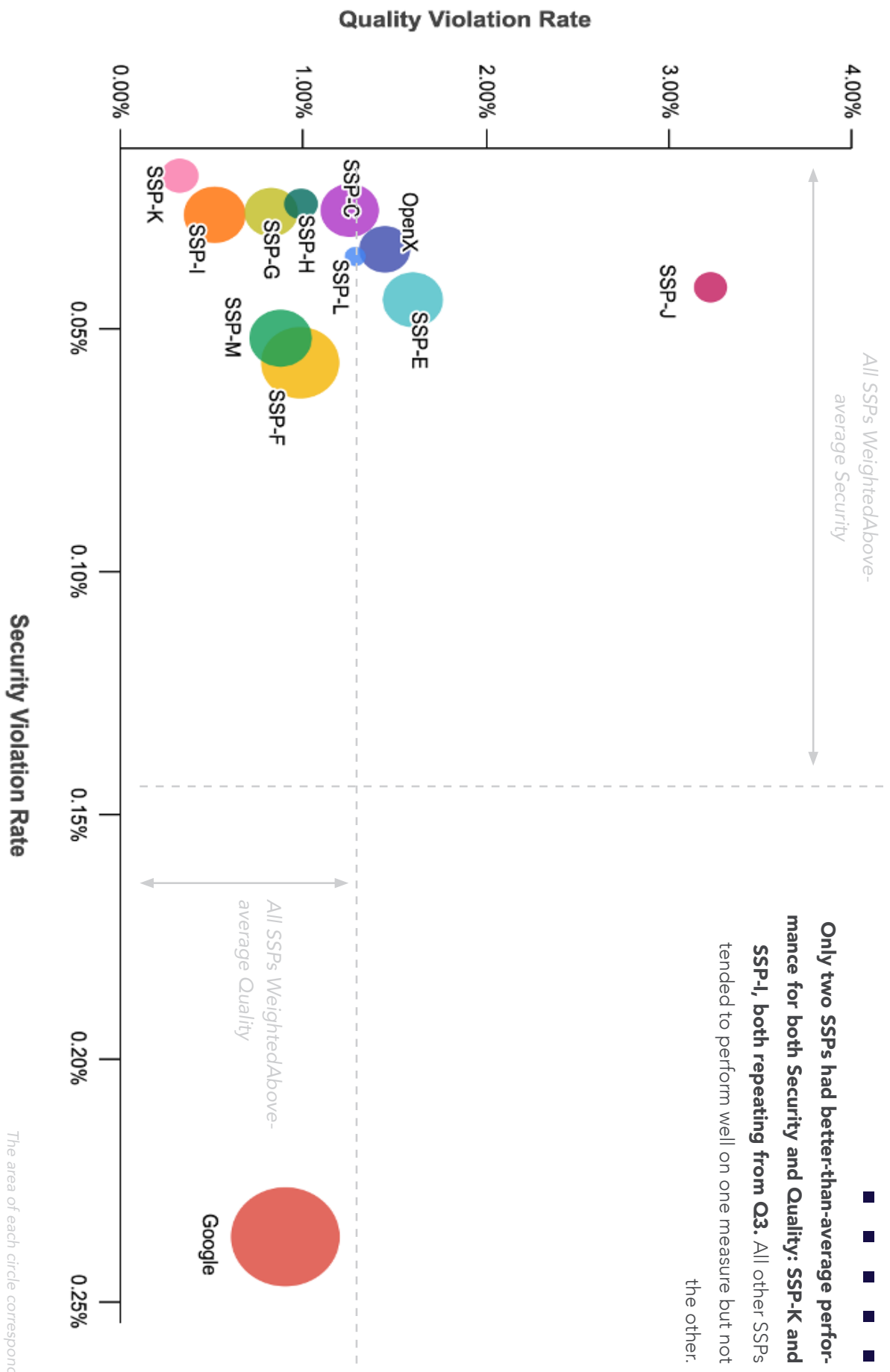
Interestingly, Google performed well in these two areas, but was the main source of ads with **Misleading Claims** (ads that use misleading language or imagery to garner clicks or sell products and services of dubious quality).



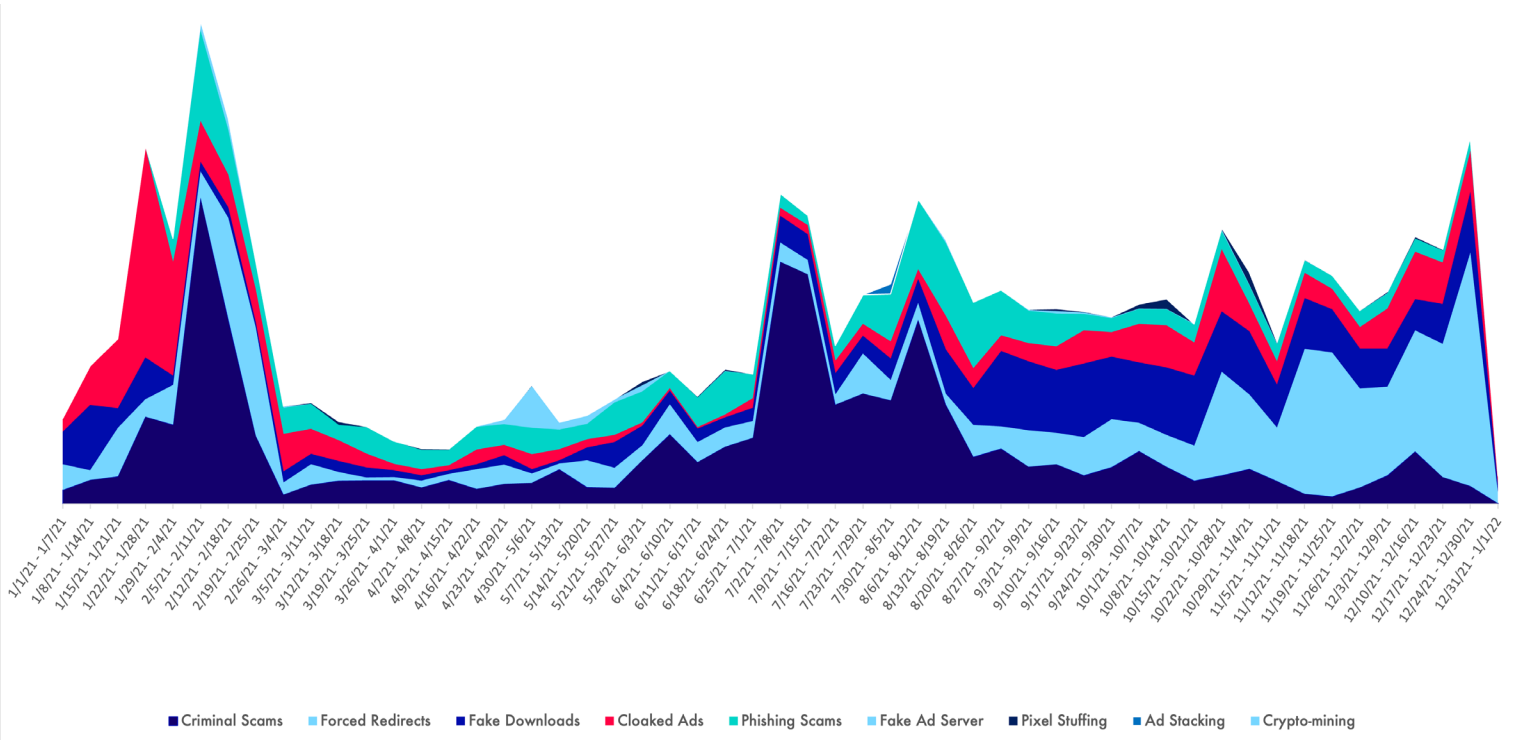
## Q4 VIOLATION RATES BY SSP SIZE

- ■ ■ ■ ■

**Only two SSPs had better-than-average performance for both Security and Quality: SSP-I and SSP-J, both repeating from Q3.** All other SSPs tended to perform well on one measure but not the other.



The area of each circle corresponds to the size of the SSP in terms of impressions delivered



## SPECIAL REPORT: PRIVACY COMPLIANCE VIOLATIONS



The nature of the Security threat shifts constantly.

**Criminal Scams** predominated in the first half of 2021.

**Fake Downloads** emerged as the top issue in September, only to be eclipsed by **Forced Redirects** in the last two months of the year.





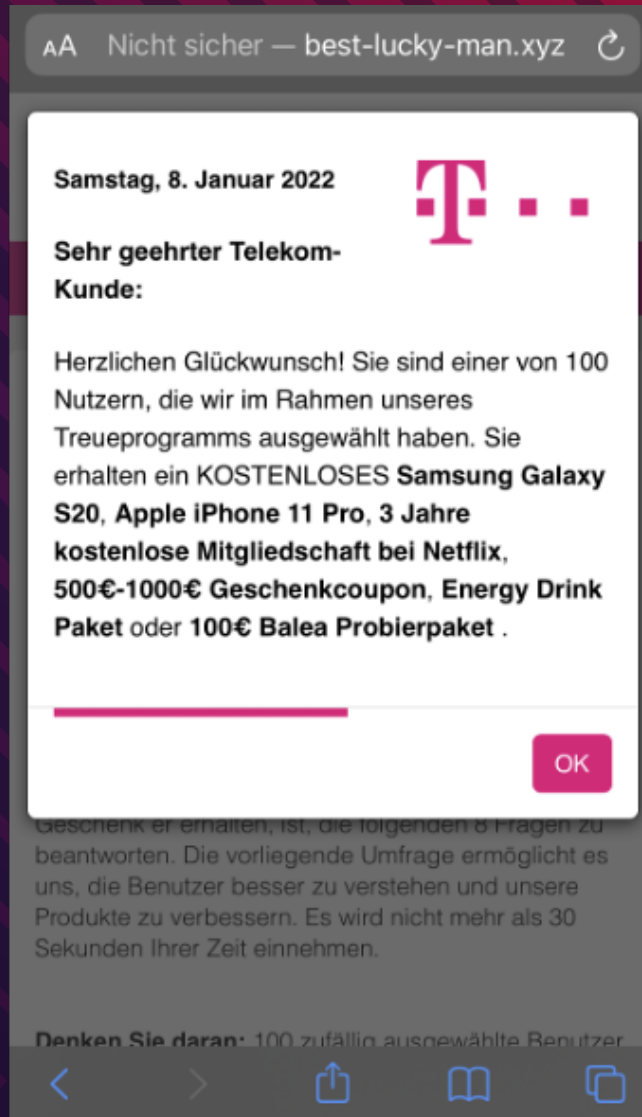
# MAJOR THREAT GROUPS ACTIVE IN Q4

---

**Q4 2021 | YEAR IN REVIEW**

MALVERTISING AND AD QUALITY REPORT





## PEAK ACTIVITY: DECEMBER

Active for many years now, ScamClub malvertisements are defined mainly by forced redirections to scams that offer prizes to “lucky” users, like the all too ubiquitous “You’ve won a Walmart gift card!” or “You’ve won an iPhone!” landing pages.

ScamClub favors a “bombardment” strategy. Instead of trying to fly under the radar, they flood the adtech ecosystem with high volumes in the hopes that the small percentage that slips through will do significant damage.

Scamclub was abusing a browser vulnerability that Confiant reported earlier in the year (CVE-2021-1801).

**LEAVING Dragon's Den To Focus On Her Investment.**

AS SEEN ON









*(Wednesday, 08. December 2021) - One of UK's top entrepreneur comes out with new secret that's making millions of Brits rich*

**(BBC)** - Entrepreneur Deborah Meaden just bought her new Mercedes using money she earned not from her TV shows - but from a

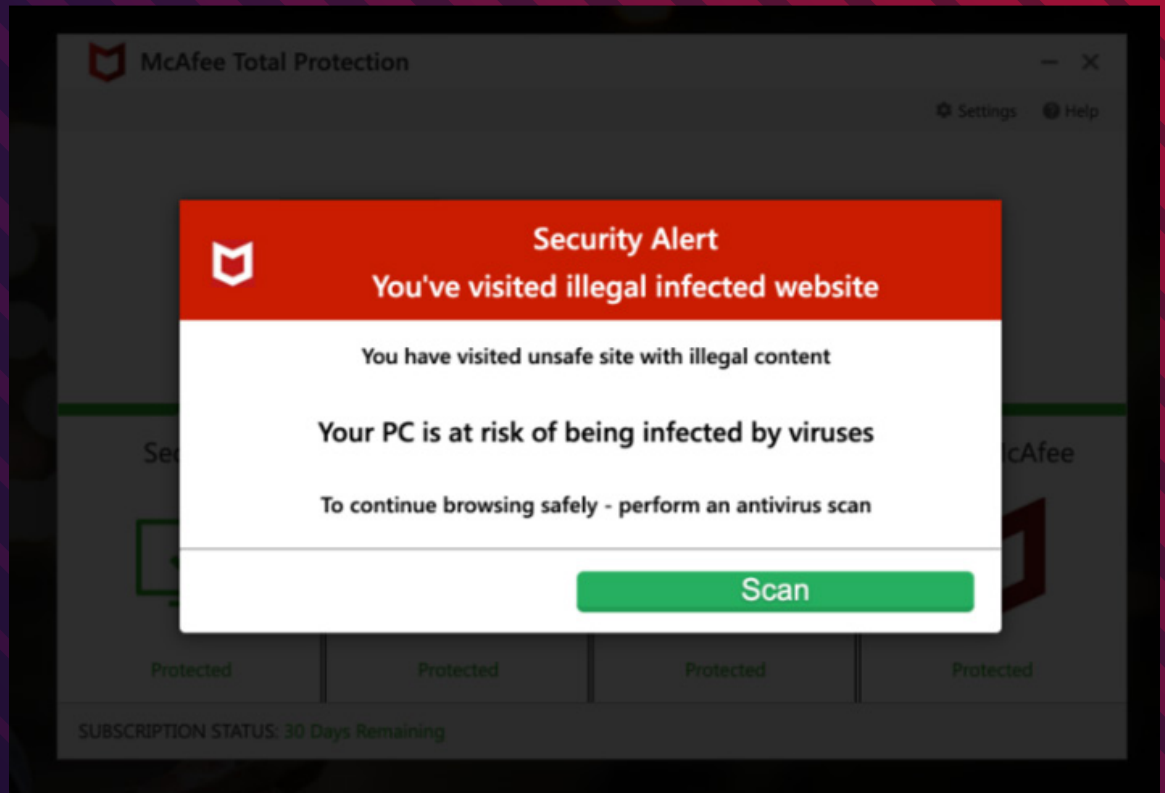


## PEAK ACTIVITY: DECEMBER

Eschewing forced redirects, FizzCore uses creative cloaking to bypass ad quality reviews and drive users to cybersecurity scam sites.

Evasion techniques include displaying fake ad creatives and landing pages to ad quality scanners, reputation and relationship building in the ad ecosystem, and carefully crafted localized campaigns using celebrity endorsement clickbait. FizzCore carefully excludes the United States from their attacks, presumably for fear of law enforcement. This is common for investment scam attacks.

# DCCBoost

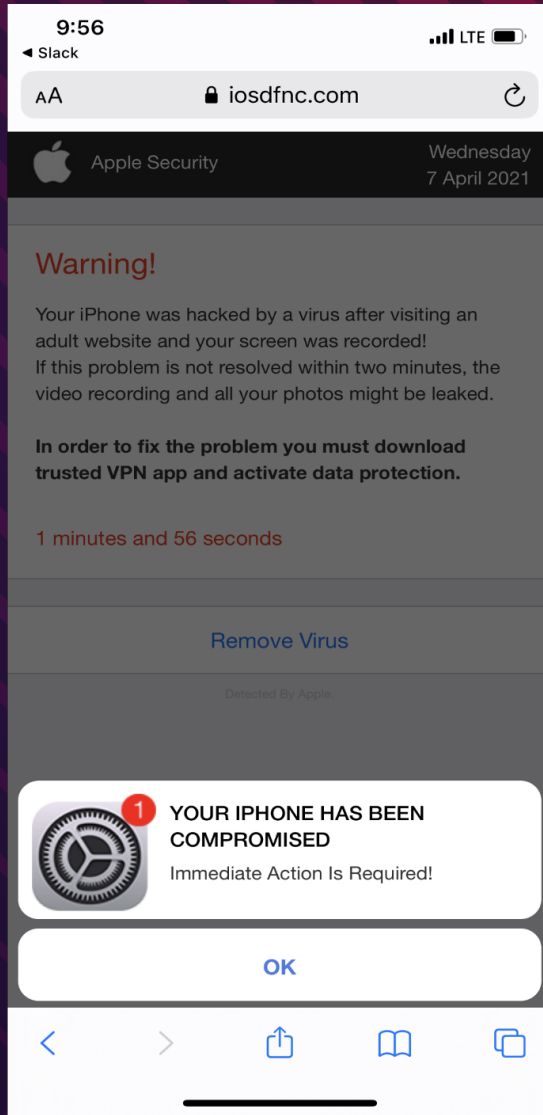


## PEAK ACTIVITY: **NOVEMBER**

Traditionally focused on mobile redirects, DCCBoost has operated a major shift after going silent since early Q3. Their new campaign forcefully redirects desktop users to a site that poses as McAfee and executes a fake antivirus scan. At the end of the scan, victims are sent to the actual McAfee site to buy the real antivirus.

As is often the case with DCCBoost, the attacks are coordinated across multiple DSPs, with a baseline activity and significant spikes.

# Tag Barnakle



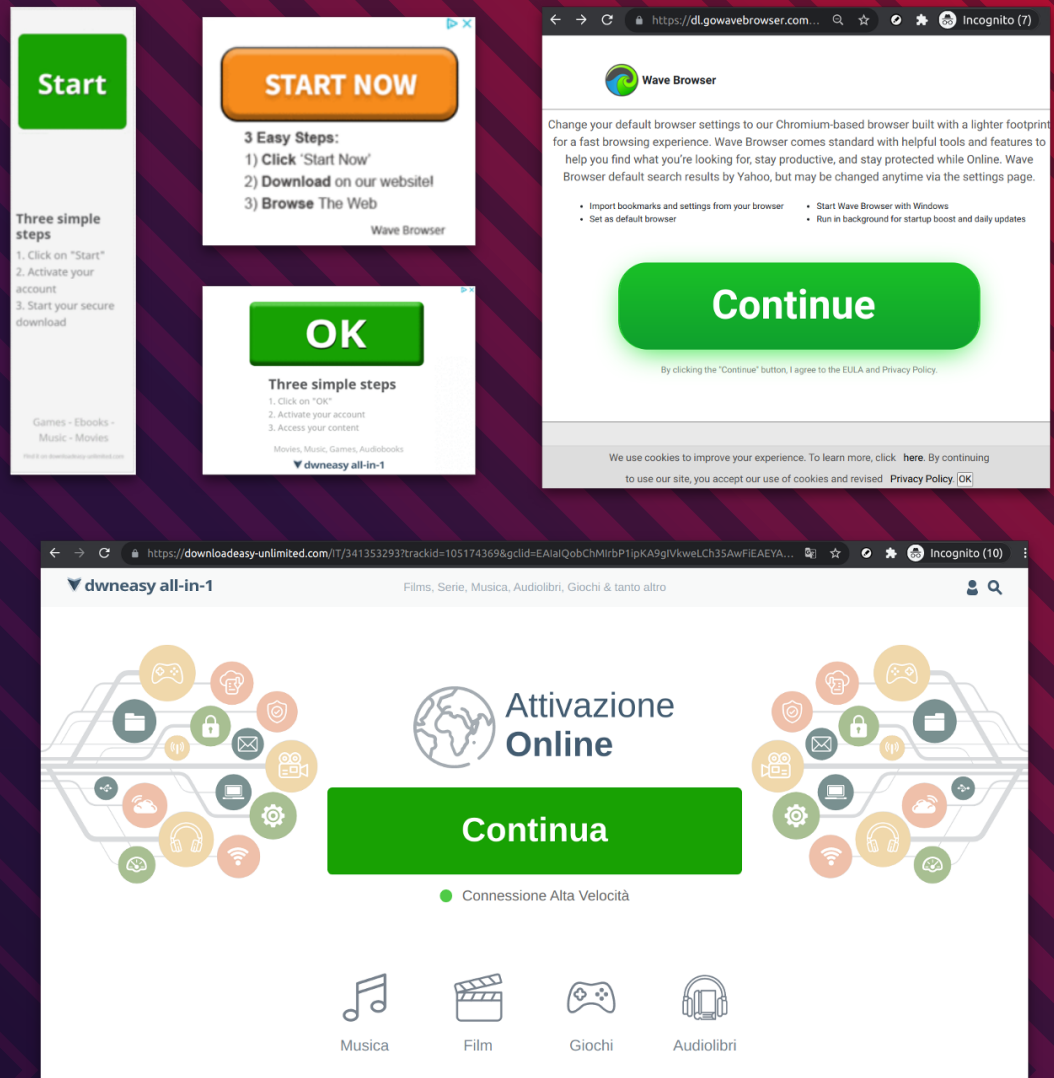
## PEAK ACTIVITY: OCTOBER

Tag Barnakle is a unique threat actor in the malvertising world that specializes in Revive Adserver compromise which they use to inject themselves into the Ad Tech supply chain without having to spend any money on media buys.

Since our first disclosure around this attacker early last year, we have seen little in the way of slow down from the group. More recently, they have re-infected an ad network that runs on top of Revive and has struggled with Tag Barnakle in the past.



# Fake Updates and Malicious Downloads



PEAK ACTIVITY:  
**ONGOING**

Fake Updates and malicious download buttons are as old as the Internet. A whole ecosystem of dubious apps and services are still leveraging this old clickbait tactic. Targeting mainly the US and Europe, they most often feature a prominent, colorful call-to-action button on a white background.

Some campaigns lead to software downloads often flagged by antivirus vendors as “Potentially Unwanted Programs” (or “PUP”) (e.g. “WaveBrowser”). Others extract subscription payments from users, while promising unlimited music, movies, audiobooks and games (e.g. “Medianess”).

These campaigns optimize to stay within ad platform policies and as a consequence are very prevalent, especially in Google Ads.



# CONCLUSION

## 2021



**We detected serious security or quality issues in one of every 125 impressions**, a significant increase from 2020.



**Criminal Scams predominated** in the first half of 2021, but were eclipsed by **Forced Redirects in Q4**.



**Friday** and **Saturday** were the days of the week with the **highest Security violation rates**, but the increase over the rest of the week was fairly modest, particularly compared to past years.

## Q4



**Violation rates for Security and Quality issues continued their upward trajectory**, matching or exceeding the previous quarter.



**Cryptocurrency became the 2nd most frequently blocked ad category** by Confiant publishers.

PARTS I, II, III

# AD-BASED FINANCIAL INVESTMENT SCAMS

By Confiant Threat Intelligence Team



We have all seen the recent stories on BBC, Guardian, CNN, Reuters, and other news outlets regarding the rise of ad-driven consumer investment scams in the UK, throughout Europe and around the world. Confiant has been tracking these types of scams for several years now. Over the past two quarters we have seen a significant increase in instances of financial investment scams victimizing people around the globe. Some areas that have been particularly hard-hit are the European Union (EU), Australia, Canada, South and Central America, South Africa, India, Malaysia, Taiwan, Hongkong, the United Arab Emirates (UAE), Saudi Arabia, and Russia. It has been particularly prevalent in areas with unstable economic conditions, where people switch to Cryptocurrencies as a protection against inflation.





## **PART I: FINANCIAL SCAMS AND MISLEADING ADS ARE ON THE RISE AROUND THE GLOBE**

The growing threat of financial scams often involves false front financial institutions that are legally registered in Cyprus (37%), **a host of other countries considered "Offshore" by Eurostat** (37%), Estonia and Malaysia (2% each), and licensed throughout the EU as investment brokers. Additionally, more than 17% of the remaining "Onshore" financial institutions identified as being involved in financial scams are either fake entities, unregistered payment intermediaries or unknown (5%). Threat actors have inserted themselves through the vector of advertising to scam your customers. These fake financial firms are capitalizing on the rise in popularity of cryptocurrencies, online trading and mobile

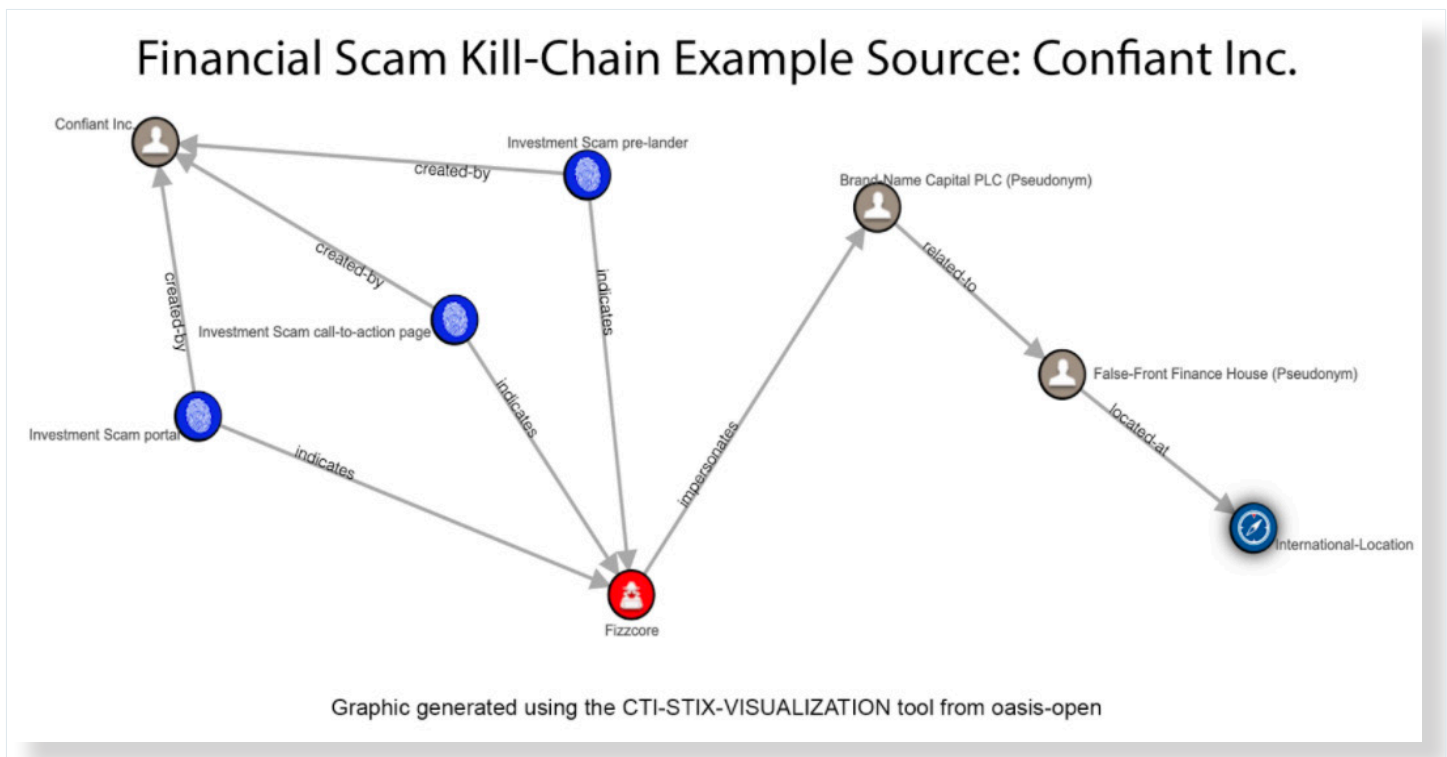
investment apps. Confiant unmasked a **financial cryptocurrency scam netting over \$1 million per day from victims**.

In our "**Financial Crime: Ad Driven Investment Scams**" document, Confiant tracked and identified threat actors who have utilized common fraudulent advertising tactics to lure their victims into disguised fraudulent investment scams. Here's an example of some user outcomes.

- **BBC News, July 29, 2021**, reported the story of Joseph (a pseudonym) who lost more than £250,000 in an online crypto currency investment

scam. He was lured into a cycle of investing more-and-more of his life savings in the false online trading scam, convinced that he was making profits. Joseph says he lost his life savings to that financial scam. His story is unfortunately far from unique. In 2018 the FTC projected that **consumers may be losing as much as \$3 billion that year in crypto scams**. Those numbers have likely been eclipsed due to the Pandemic. **“Recent Victims of a prolific bitcoin scam are reporting individual losses of up to**

as she deposited it. **Her attempts to have the Australian Cyber Security Centre (ACSC) and the Australian Federal Police’s operations monitoring centre, and the Western Australian Police take action were largely unsuccessful.** The police traced the transactions to banking resources in Eastern Australia and then to an entity registered to a bogus financial investment firm registered in Saint Vincent and the Grenadines.



**£200,000 after following links on AOL, MSN, Yahoo and Facebook**

- **ABC News, September 19, 2019**, reported the story of Bunbury Australia resident, Jane Smith (a pseudonym), who lost \$670,000 through an ad-based financial scam. The bogus ad was made to look like an authentic ABC News story of the famous Australian mining billionaire, Andrew Forrest’s latest miracle investment. This ad and many like it using other faked celebrity endorsements are posted on Facebook, LinkedIn, Instagram, and other trusted websites. The scam ads are supported by authentic looking financial websites with related articles that support the fraudulent scams. Her money was lost as soon

**SCAMS HAVE MORPHED FROM CRYPTOCURRENCY TO “FALSE FRONT” INVESTMENTS**

More recently, we have seen the threat actors go beyond crypto-scams to the creation of advertising for false front EU investment firms that appear legitimate. But their ads hijack the names of trusted brands like **Netflix, Amazon or famous celebrities like Elon Musk**, to lure investors into their scams that steal their personal information or draw them directly into a financial scam. Consumers in the United Kingdom have been especially heavily targeted, though we have observed these financial scams throughout the EU and in many other countries. The scams are a significant financial threat to EU consumers as potential victims. TNW




This is a graphic representation of the Confiant STIX v2.1 financial scam kill-chain example. Graphic generated using the CTI-STIX-VISUALIZATION tool from oasis-open, ref: <https://oasis-open.github.io/cti-stix-visualization/>

## SOPHISTICATED FRAUDSTERS DESIGN ELABORATE FINANCIAL SCAMS

Most of the fraudulent investment firms operate at the end of an elaborate “kill-chain” responsible for a large amount of the current malvertising investment scams. According to victim’s complaints, the fraudulent investment firms are reportedly responsible for a wide variety of unsavory practices that are discussed in Confiant’s, “[Financial Crime: Ad Driven Investment Scams](#)” and associated briefing. In it, we dubbed one leading financial scam threat actor [HircusPircus](#). They are financially and technically savvy as well as ruthless. Their scam usually starts with ads offering investment opportunities in well-known, high-performing companies or cryptocurrencies. Their ploys include customized entry point ads, pre-landing pages, entry forms to gather user personal data, and scam investment portals and payment pages (sometimes third-party payment sites) that make it appear like the victims are making profits on the invested funds through their fraudulent portal.

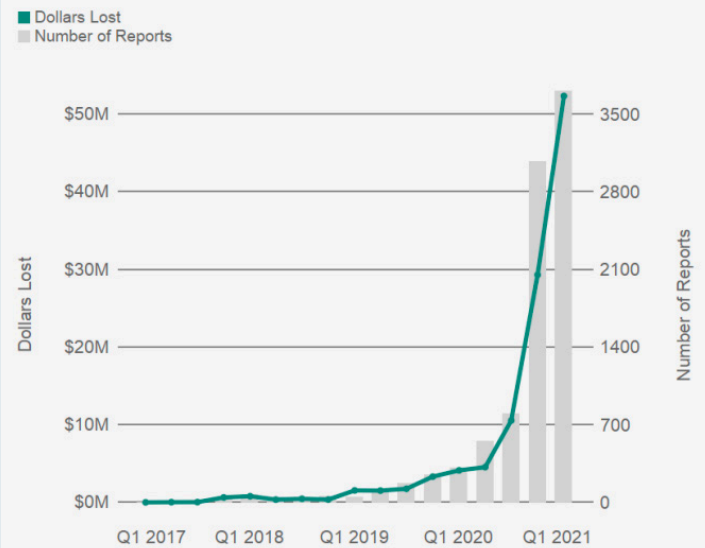
Confiant’s ongoing threat intelligence work maps some of the tactics in the entire kill-chain of HircusPircus, as well as tracking several other active threat actors that Confiant has previously identified. Increasingly complex scams by the emboldened scammers have gone beyond Europe to other parts of the world as well.

But, the story doesn’t end here. In our discussion of [Financial Investment Scams Part II](#), we will explore the deeply deceptive world of financial scams, their global reach, some of the types of ads they use to hook consumers, and what financial fraud departments can do about it. 

## PART II: THE US AND AUSTRALIA REPORT HUGE INCREASES IN FINANCIAL SCAMS

### Reports and reported losses to cryptocurrency investment scams increased sharply from October 2020 through March 2021

Number of cryptocurrency investment scam reports and reported dollar losses by quarter (Q1 2017 - Q1 2021)



These figures are based on reports to the FTC’s Consumer Sentinel Network that were categorized as investment related fraud and indicated cryptocurrency as the payment method.

The US Federal Trade Commission report. Note the sharp increase of investment scams over the last year.

### The US Federal Trade Commission (FTC)

reported that “Since October 2020, reports have skyrocketed, with nearly 7,000 people reporting losses of more than \$80 million on these scams. Their reported median loss? \$1,900. Compared to the same period a year earlier, that’s about twelve times the number of reports and nearly 1,000% more in reported losses.”

On [January 5, 2020](#), [ABC News Australia](#) reported that Australians lost more than \$86 million to financial scams, more than any other form of criminal scam. On [August 24, 2021](#), [The Australian Competition & Consumer Commission \(ACCC\) ScamWatch](#) reported that investment scams cost Australians over \$70

million in the first half of the year alone, exceeding the total reported losses for all of 2020, with projected losses expected to reach \$140 million by the end of 2021. Australians submitted 4,763 reports of financial scams in the first six months of 2021, which is a 53.4% increase in comparison to the first half of 2020. More than half of the reported \$70 million in losses was due to Bitcoin and other Cryptocurrency scams. Bitcoin losses in the first half of 2021 were estimated at \$25.7 million, up 44% from the \$17.8 million total scammed in all of 2020. The ACCC Scamwatch received reports of more than \$1 million lost to financial ponzi scams that started with social media ads, linking to mobile apps such as "Hope Business" and "Wonderful World" until they were finally removed from official app stores. [ASIC executive director for assessment and intelligence Warren Day](#) said that the minute that funds are transferred to a financial scam site, they are moved to another account in different country, and that cycle repeats to make it very hard for regulators and money tracking authorities such as AUSTRAC to identify where the funds have gone.

Lead-in bait to these scams includes: investment in cryptocurrency, mining of cryptocurrency, celebrity give-away scams, investment in stocks and imposter bond shares of hijacked brand name companies, ponzi schemes, online dating and romance scams, and scammers that say they represent government agencies (like the Social Security Administration, the Internal Revenue Service, etc). On December 10, 2020 the FTC issued a report that said the COVID-19 pandemic had created ideal conditions for an increase in [scams including fake "training" scams for online investing and real estate with reported median individual losses of \\$16,000 each, and \\$24,000 for people in their 50s and 60s](#). The same report indicated that many who were drawn into financial pyramid scams were first contacted through social media such as [Facebook, Instagram, LinkedIn, Pinterest, Reddit, Snapchat, TikTok, Tumblr, Twitter, or YouTube](#).

### **CRYPTOCURRENCY IS THE "PERFECT STORM" FOR SCAMMERS:**

Cryptocurrency is used as both the bait and a shield for many scammers. Scammers may start by requesting small deposit amounts on victim's credit cards but then move lured victims to wire transfers for larger amounts. By scammers insisting on

cryptocurrency for payments, the victim is left **with fewer avenues of remediation**.

### **Here's what the FTC says about Cryptocurrency and Scams:**


- "Cryptocurrency doesn't come with legal protection like credit or debit cards (or other traditional forms of financial payment). Credit cards and debit cards have [legal protections](#) if something goes wrong. For example, if you need to [dispute a purchase](#), your credit card company has a process to help you get your money back. Cryptocurrencies typically do not
- Payments made by cryptocurrency are not reversible, unless the individual or organization you sent the payment to, sends it back.
- Some information about cryptocurrency transactions is recorded on a public ledger, called a blockchain. A blockchain is a public list (a database or ledger) of every cryptocurrency transaction - both the payment and receipt sides. Depending on the cryptocurrency, the information added to the blockchain can include details like the transaction amount and the sender's and recipient's wallet addresses. A wallet address is a long string of numbers and letters linked to your digital wallet (like a bank routing and checking account number). Even though you can use a fake name to register your digital wallet, it's possible to use transaction and wallet information to identify the people involved in a specific transaction. And when you purchase something from a seller who collects other information about you, like a shipping address, that information can be used to identify you later on."

The combination of these factors creates an environment that is highly favorable for scammers and their unsavory practices. By paying with cryptocurrency, consumers lose the legal protections that other more traditional financial methods offer, like fraud departments at those financial institutions who can pursue complaints. Without reversibility, it is even harder to retrieve scammed funds, even when the scam is identified. And, because more of consumers' personal information is shared on the public blockchain ledger, consumers are exposed to threat actors who want to use that personal information to commit identity theft or other types of targeted fraud.

## AD SECURITY THREAT INTELLIGENCE COULD BE AN EARLY WARNING SYSTEM:

Confiant is committed to help identify and disrupt this type of financial scam by working with our partners in financial institutions as well as our existing clients. Confiant's ad security threat intelligence includes information regarding the organizations involved in scams, where it is available. The information, if used proactively, could empower a bank or financial institution to block transfers of funds to unsavory institutions in advance of the money being stolen, disrupting the kill-chain, and protecting their customers. Customers often look to their bank or financial firm for help to rectify debt incurred in scams or recover losses due to financial scams after they occur. Confiant may be able to help as an early warning system for the bank's fraud department to prevent losses before they are completed.

Confiant created the world's leading cyber security solution to identify, block and protect against ad driven threats. The comprehensive protection from malvertising, disruptive ads, and privacy violations inside the ad ecosystem Confiant's proprietary ad security threat intelligence may assist bank and finance companies' fraud

prevention departments outside of the ad tech industry. This represents a deepening of Confiant's mission as we extend the spheres where we can protect from the Malvertising threat actors at other points in the kill-chain. Confiant's ad security solution helps the advertising ecosystem, giving publishers and ad platforms better filters over what flows through their digital pipes. If the potential fraud information is shared with the fraud prevention departments of retail banks and other financial institutions, it may help them to halt any funds transfer before these malicious scams victimize their customers. For more information contact us to receive our: "Financial Crime: Ad Driven Investment Scams" briefing. 



## PART III: WHAT IS BEING DONE TO PREVENT AD-BASED INVESTMENT SCAMS?

In [Part I](#) and [Part II](#) we discussed how Ad-Based Investment Scams have become a worldwide problem with significant losses to individuals, very few laws regulating these scams, and lagging actions by authorities and financial institutions; all of which leaves law enforcement and fraud departments with minimal incentives, or the authority, to take action. Now we will examine what organizations are attempting to do about the problem and what else can be done.

### COMPLEXITY OF INVESTMENT SCAM DESIGNS

Criminals who design ad-based investment scams are very sly and devious about their designs. They are fully aware of the possibility that their scams may be discovered and stopped at any point during the scam. So, they created redundant designs that can recover or

can be easily rebuilt whenever they are discovered or stopped. Those designs also draw in anyone trying to stop them to "Whack-A-Mole" situations (a game that is designed to make them lose), where new scams appear as fast as old scams are stopped.

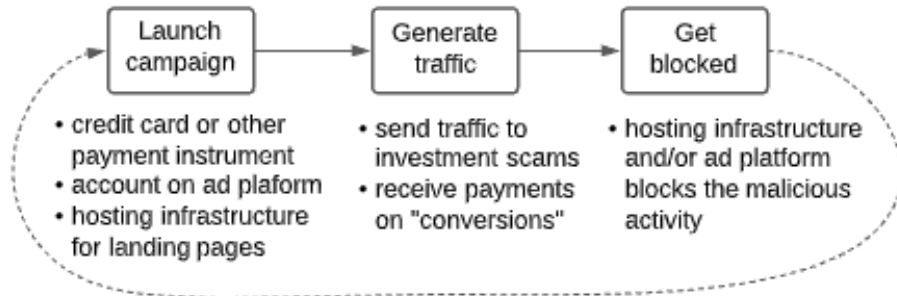
The first section of the design is the advertising loop that we call the "Ad Whack-A-Mole" because of the difficulty it creates in stopping and eliminating the ads that lead to the scams. The second section is the Legal Entity Factory or "Financial Whack-A-Mole" as we call it because of the difficulty it creates in stopping and eliminating financial fraud. Each loop is designed to make it difficult for responsible ad tech and banking fraud prevention departments to find and stop the false-front ads, the fraud activities, and the actual transfers of funds from victims. Whenever a portion of the scams actually do get blocked, threat

# The Financial Crime Double Whack-A-Mole

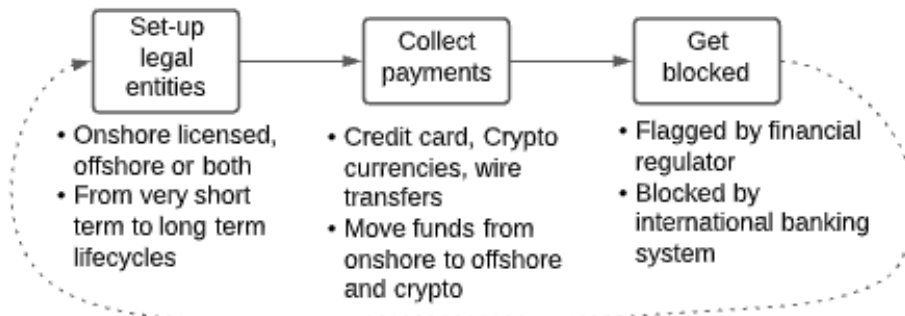
Source: Confiant



## The Ad Whack-A-Mole: Scaled attacks with paid traffic



## The Financial Whack-A-Mole: Legal entity factory



- **Attackers are ready to immediately rebuild their infrastructure**
- **Each iteration is a learning opportunity to maximize persistence and react to defensive measures**

© 2021 Copyright Confiant Inc. All rights reserved.

Whac-A-Mole is a trademark of Mattel Inc.

All other trademarks are the property of their respective owners.

actors recreate a slightly different ad or financial entity with nearly identical functions as the previously blocked scam, and they start the loop over again. Each loop is designed to be autonomous but acts in unison, in order to hide identifying that they are linked.

## THE AD COMMUNITY'S PART

As with many problems facing the marketplace, there are often many different viewpoints on how to fix the problems and who is responsible, or who is in charge of implementing those fixes and

remediations. The advertising community has long been aware of the ad-based financial scam issue. Over the last few years the news media has exposed that the rate of occurrence of scam ads is on the rise as is the quantity. It would be difficult for any Platform, Publisher, or even well-known celebrities to say that they are not aware of the issues as all have been affected or accused of somehow being involved in these scams. Not only have cases and incidents become well publicized, but most have received complaints from victims who were scammed out of funds, because they couldn't differentiate between the malicious scam or cloaked ads, and legitimate



ads with both rendering side-by-side on the same well-known and trusted websites. The same can be said for legitimate endorsements from those same celebrities. The victims either trusted the website where they viewed the ad, or the representation of a trusted celebrity name or face before they clicked through to the scammer's trap. Either way, the scams clearly degrade the reputations of websites and brands that are reliant on legitimate advertising revenues as well as causing loss of trust from their audiences. That has impacted the reputations and revenues of the advertising community.

Recently, Google announced that they will require that [any company advertising financial services on the Google search engine \(in the UK\), must be authorized by the Financial Conduct Authority \(FCA\)](#). While this sounds like an admirable first step, considering the fact that Google is the largest ad tech platform in the world, this is indeed a very small step focused only on the UK audience, not the entire public Internet where Google's search engine dominates. Also, Google's new requirement only affects those ads actually offering financial services within the ad itself (only a portion of the scam ads actually advertise financial services, many others draw victims to the threat actor's websites where offers of financial services are not easily observed).

The results? Since the Google announcement, the quantity of ads with security violations, [many leading to financial scams, has increased within the UK](#) as well as worldwide. Unfortunately predictable given the arms race nature of the cyber security cycle where every action, even preventative ones, will attract more sustained attention from an ever larger group of bad actors who interpret attention as opportunities for malicious profit. In our [Malvertising and Quality Index \(MAQ\) report for Q3 2021](#), Confiant reported that the overall worldwide ad security violation rates nearly tripled over the prior quarter's rate, now the highest level in over a year. The MAQ reported large increases in ad security violations over the Q2 2021 rates throughout Great Britain, France, Spain, and Germany. For that period, Google's worldwide sell side (SSP) ad security violation rate exceeded the industry average by 48%. While many of the other top SSP security and quality violation rates in the same report showed improved vigilance around reducing those violations, Google slipped into second from last place among top SSPs, as due

to their size they have borne the brunt of this new attack cycle. [A recent MIT Technology Review](#) found that tech giants Facebook and Google are paying millions of ad dollars to bankroll clickbait actors with their engagement-driven algorithms that amplify and monetize inflammatory content, fake news, and misinformation, fueling global misinformation though, so the reality is more nuanced than this just being about the bad actors going after the biggest until their defenses catch up. The Ad Ecosystem has the ability to prevent ads with security violations from appearing on sites, but they need to change their tactics and employ technology that creates transparency and control if they wish to combat the malicious ads.

Some Publishers and Ad Platforms in the community had begun to tackle the problem, by implementing ad threat intelligence reporting and blocking solutions in order to prevent the scam ads from appearing on their websites. The attackers had until recently focused primarily on compromising display ads, but over the past two years malicious activity has surged in all the other media channels too (search, social, native, video etc). Depending on the technology and expertise of the threat intelligence solution implemented, scam ads that lead to financial scams aren't always recognized or exposed. Because, as discussed earlier in this blog post, the ads themselves do not always trigger ad security alerts and may be considered safe by typical ad threat scanner solutions. It takes a well-designed, savvy combination of real-time scanning technology, as well as seasoned expertise and knowledge of the solution designer threat intelligence staff to create a solution that automatically identifies the most dangerous scam ads.

Those that have implemented the best solutions and the best practices have already delivered protection to their users and achieved reduced ad security violation rates that are lower than industry averages, even during periods of increasing worldwide security violation attacks. Individual cases are identified in [Confiant's ongoing MAQ report series](#).

## THE GOVERNMENT'S PART

Different government entities vary in their approach and enforcement of ad-based financial scams around the world. In 2016, the UK created and launched



the [National Cyber Security Centre \(NCSC\)](#), to help make the UK the safest place to live and work online.

This is part of the UK's attempt to thwart online security threats. But, fast-forward to articles like this one in the [Economist, November 27 2021 "Scams and fraud are criminally under-policed in Britain"](#) are still reporting increases in criminal activities with limited police activities to counteract the increasing onslaught of criminal scams. Government activities have not been without results though, with multiple different reports in [January 2022](#) stating that the Russian intelligence service (FSB), in cooperation with reports from United States threat-intelligence identifying the culprits in several high-profile ransomware attacks, arrested the suspected leaders of the notorious international ransomware gang REvil. The Russian FSB and Russian Ministry of Internal Affairs statement indicated that their combined efforts have neutralized the information infrastructure of that criminal organisation.

Tangential to ad-based investment scams, the UK's [Action Fraud](#), national reporting centre for fraud and cyber crime, revealed on November 22, 2021 that 28,049 shoppers were scammed out of approximately £15.4 million when shopping online over the prior 2020 Christmas period. That's in addition to the £1.6m lost to online charity fraud scams during 2020, reported by the [Fundraising Regulator](#), the [Charity Commission for England and Wales](#), [National Trading Standards](#) and [Action Fraud](#), who joined forces to warn the public of ad-based charity scams, which increase every year during the Christmas Holiday Season.

On [October 13, 2021](#) the [US Federal Trade Commission \(FTC\)](#) included a clear message to any businesses that pitch money making ventures, that if they deceive or [mislead consumers regarding potential earnings](#), the [FTC will be ready to hold them responsible](#) with every tool at its disposal. This lays the foundation for US enforcement authorities to

pursue financial scams advertised to the public.

In Australia, some regulatory entities have begun to hold businesses accountable for losses of consumer personal information and financial fraud losses, if they do not adequately protect those consumers from fraud or safeguard their data. The Australian regulatory entities include: [Australian Competition and Consumer Commission \(ACCC\)](#), [Australian Securities and Investments Commission \(ASIC\)](#), [Office of the Australian Information Commissioner \(OAIC\)](#), and [Australian Cyber Security Centre \(ACSC\)](#) among others. In addition, Australia has created laws against paying ransom to cyber criminals under their [AFP](#), [DFAT](#), [CDPP](#) laws.



Well-known celebrities have joined forces to object to the use of their likenesses and names (or brands) being used in these scams by demanding that the UK Prime Minister, their government and law enforcement take action against the fraudsters and the malvertising.

In November 2021, [MSE News](#), [NewsChain](#), the [Metro](#) and others reported that Martin Lewis, Sir Richard Branson, Deborah Meaden and other public figures issued a plea to the UK's Prime Minister to put scam ads in the Online Safety Bill.

## THE BANK'S PART

According to the banking trade body UK finance, there was a [71% increase in reported cases of financial scams in the first half of 2021 over 2020](#) amounting to more than [£355 million in total losses](#). [Criminal scams accounted for £4 million in daily losses for the first half of 2021](#).

In the UK there is a [voluntary program that was instituted in 2019](#) whereby participating banks will reimburse their patrons who became victims of Push Payment Fraud (which includes the Ad-Based Financial Scams discussed above). However, in a [November 18, 2021 Daily Mail article](#), there were

several reported instances where the same banks that joined the voluntary program were not actually treating scammed customers fairly, and issues took several months to be settled by the UK Financial Ombudsman. In some cases, banks offered less than half of the stolen funds to customers or rejected their claims completely, based on the bank's interpretation of the regulations of the program. The Daily Mail article reports the case of an elderly couple, the Brodies, who were scammed out of £21,000 by scammers posing as banking employees. Their bank offered only half of that amount in reimbursement, and the Brodies had to wait eight months before their complaint through the Financial Ombudsman finally settled in their favor.

As a result, some authorities in the UK have begun to create regulations that will hold financial organizations responsible for the mandatory replacement of funds lost to victims of financial scams if the organizations do not adequately protect and warn consumers in advance of being scammed. Those financial organizations include banks, building funds, credit card companies and some financial institutions. Regulatory authorities changed from a voluntary to a mandatory program in order to make financial institutions become fiscally responsible for the problem. They want financial institutions to take action as well as responsibility to protect their own customers and also do more to prevent the financial scams and fraud. Those recent changes in the rules of the program will now make reimbursement by banks for their scammed patron's losses mandatory, and may also include fines if the banks are not treating customers fairly. The new mandatory program will force UK financial institutions to have financial "skin in the game".

**For more:**

Speak with Confiant's Threat Intelligence Team

**[EnterpriseSecurity@Confiant.com](mailto:EnterpriseSecurity@Confiant.com)**



# ABOUT CONFIANT

Confiant's mission is to make the digital world safe for everyone. We defend the digital ad industry by helping publishers and ad platforms protect their users and take back control of the ad experience from rogue actors. Our solution protects reputation, revenue, and resources by providing real-time verification of digital advertisements.

By providing industry-leading protection from malvertising, disruptive ads, and privacy risks, Confiant empowers premium ad platforms and publishers with actionable data to ensure the digital ad ecosystem is safe and secure for everyone. We protect hundreds of billions of impressions per month for our clients, which include CBSi, Magnite, Gannett, Politico, and as a trusted Amazon Publisher Services, Connections Marketplace vendor.

**LEARN MORE: [confiant.com](https://confiant.com)**





MALVERTISING + AD QUALITY INDEX

# MAQ INDEX

---

[CONFIANT.COM/MAQINDEX](https://confiant.com/maqindex)

For more information on our entire suite of Security, Quality and Privacy protection products please visit our website or

email us at:

[MARKETING@CONFIANT.COM](mailto:MARKETING@CONFIANT.COM)

---

**Q4 2021 | YEAR IN REVIEW**

MALVERTISING AND AD QUALITY REPORT