Arkose Labs

Digital Media and Streaming

Q3 2020 Fraud and Abuse Report

Introduction

The digital media industry continues to see consistent levels of fraud. In particular, this is a sector that sees a high amount of attacks come via the mobile channel. 54% of attacks targeting media companies are on mobile transactions, which is a much higher that the 21% average across all industries on the Arkose Labs network.

This isn't surprising since digital media is mobile-friendly, and many of the platforms are app-based. Media platforms are known for simple and easy sign-up processes and quick and seamless authentication on-the-go. This makes it an attractive sector for fraudsters to attack.

In particular, social media saw a large spike in bot-driven fraud activity in April and May, with automated attacks used primarily to scrape information, launch scams or disseminate malicious content. As we move on into 2020, this will continue to be a trend to watch. A presidential election in the U.S. could spur even more bot activity on social media platforms in order to influence public opinion and spread so-called "fake news."

By better understanding the evolving digital landscape, businesses can ensure they are well-equipped to tackle the rising tide of fraud and ensure long-term protection against attacks.

1H 2020: Key Fraud and Abuse Trends

As COVID-19 forces commerce online, the Arkose Labs network records double the volume of attacks over 6 months.

1.1 billion
attacks detected and stopped

2x attack volume
since 2H 2019

25% attack rate
on all transactions

Elevated Attack Levels in 2020

Attack patterns have been evolving rapidly in the first 6 months of 2020

21.2% mobile
attack mix

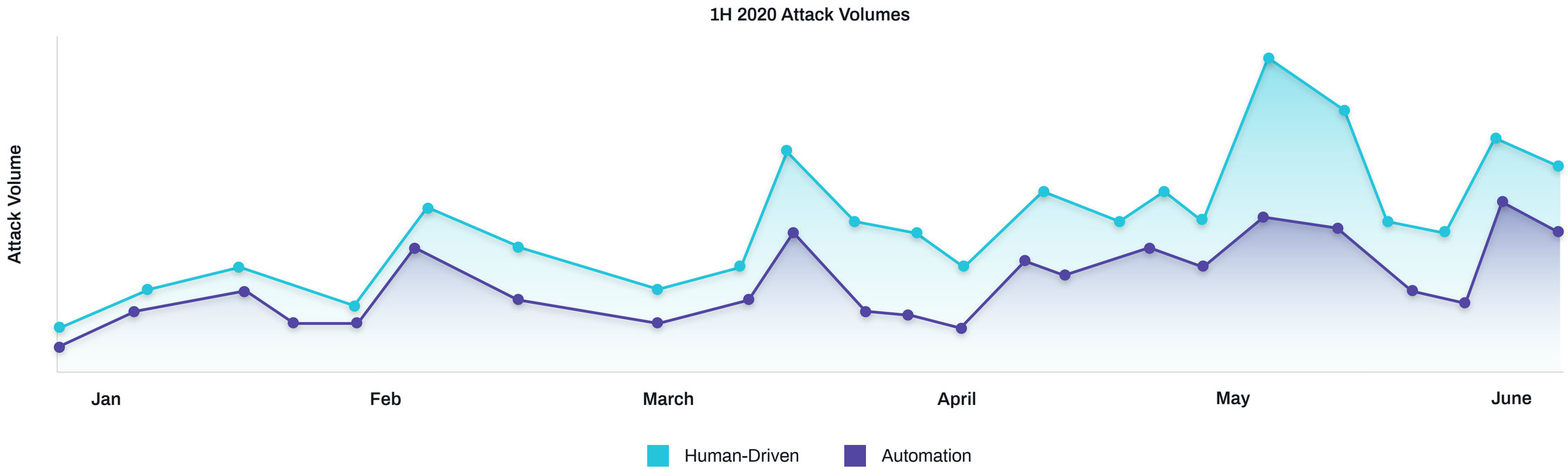
33.5% human
vs 66.5% bot attacks

Most attacked
use case is logins

Heightened Attack Volumes in 2020

Businesses are facing an increasingly hostile threat landscape in 2020. Major spikes in attacks can be seen across the first six months of the year,and Arkose Labs has observed a general upwards trend in the intensity of attacks. Normal consumer behavior has been in flux, due to the upheaval caused by COVID-19. It is harder to user historical benchmarks of transaction habits when assessing traffic.

Therefore, organizations relying purely on data-driven fraud defenses run the risk of more traffic falling into a "gray area" when differentiating between trusted and fraudulent behavior. They therefore require robust defenses that provide hard evidence of a user's true underlying intent.



Media Companies Face Mobile and Sweatshop Attacks

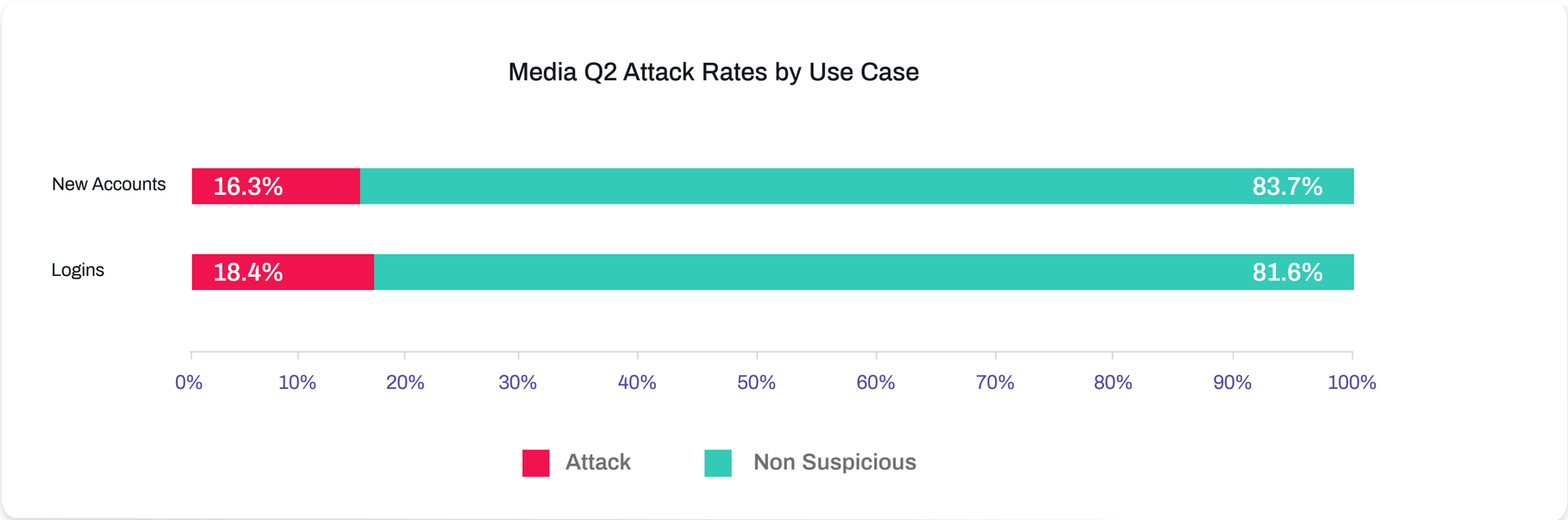
17.8%
attack rate

25.5% of attacks from sweatshops

39% of attacks on mobile

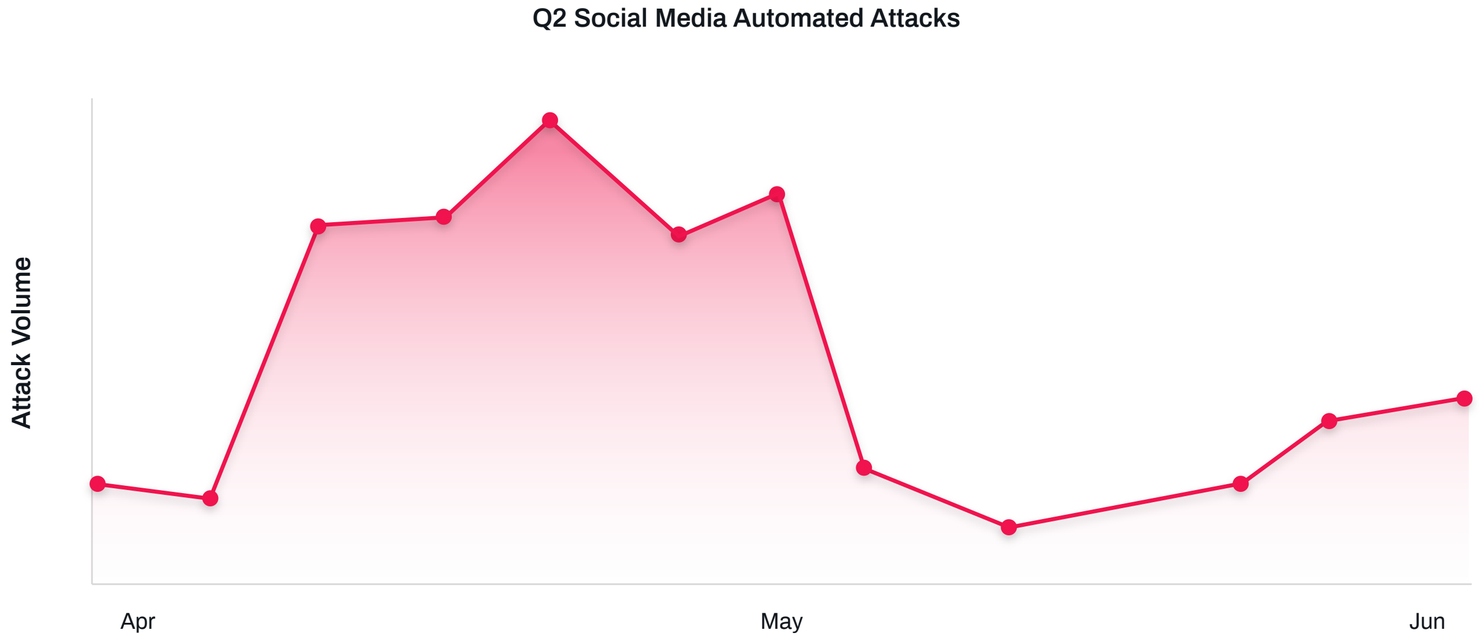
Digital media, streaming and social media companies are major targets for card testing, abuse of free trials and reselling of paid accounts. Without the correct tools in place, companies face major hurdles in stamping out abuse without spending manual time identifying bogus or compromised accounts.

The media industry has high levels of mobile traffic. As a result, it sees elevated mobile attack rates. 39% of attacks targeting media companies are on mobile transactions, which is a higher proportion than any other industry. This was particularly elevated in Q2, with mobile attacks up 31.5% compared to the previous quarter.



The Scourge of Bots in Social Media

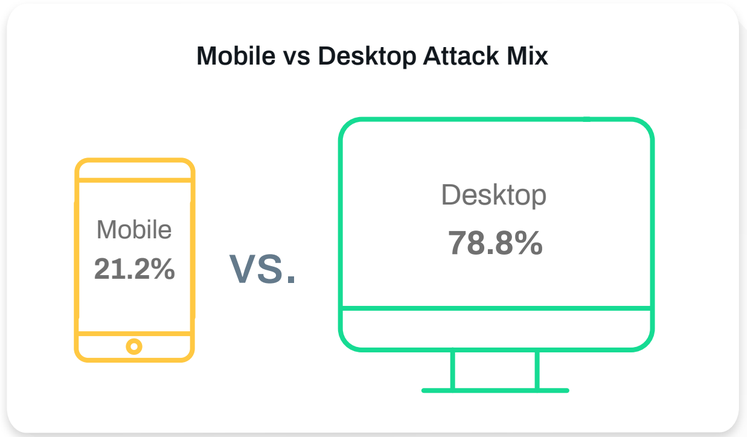
Social media sites saw a spike in bot-driven activity in April and May. Bad actors use bots across a variety of social media platforms in order to scrape information, launch scams or disseminate malicious content. Bots are deployed in attempts to influence political and social discourse by spreading information en masse and carrying out hashtag hijacking and trend-jacking. This issue of bots within social media will continue to come under great scrutiny in the second half of 2020, as debates over COVID-19 safety measures and a presidential election in the United States dominate public discussion.

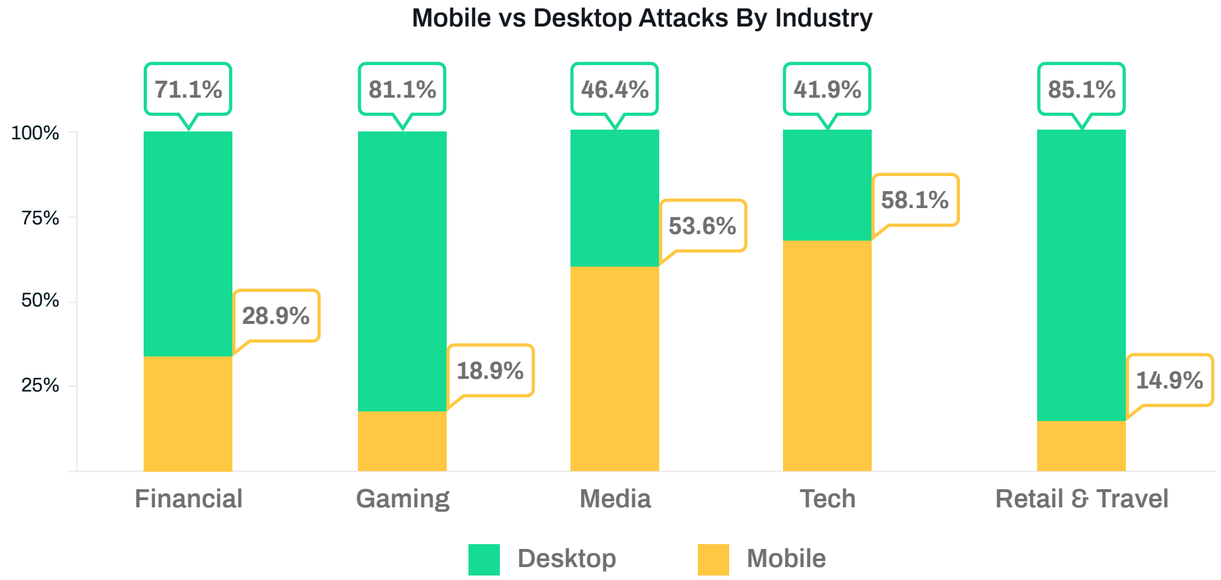


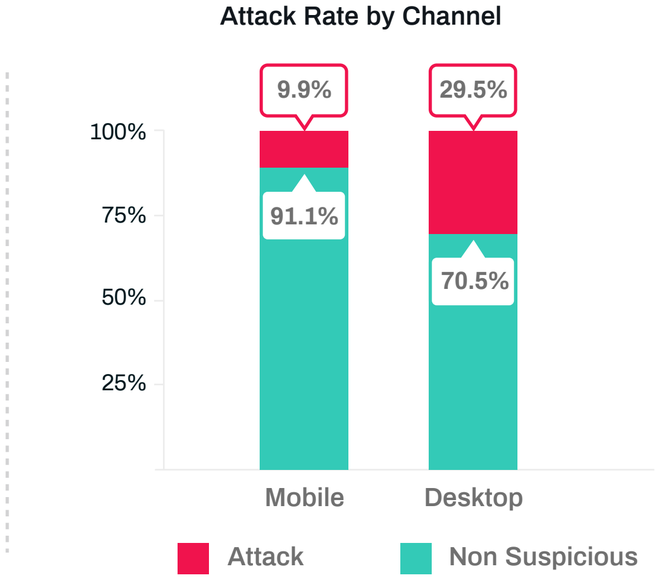
Mobile Powers Sweatshop Attacks

While mobile attack rates vary greatly by industry, overall they are lagging behind desktop attacks on the Arkose Labs network. 37% of all transactions originated from mobile, but only 21% of all attacks were on mobile transactions. Of those mobile attacks, 38% were human-driven which is higher than the overall human-driven attack mix. Click farm workers will line up multiple mobile devices to execute attacks at scale.

There is a great deal of variation in the mobile versus desktop attack mix when parsing this by industry. Media (including social media) and technology saw a majority of their attacks targeting mobile transactions.

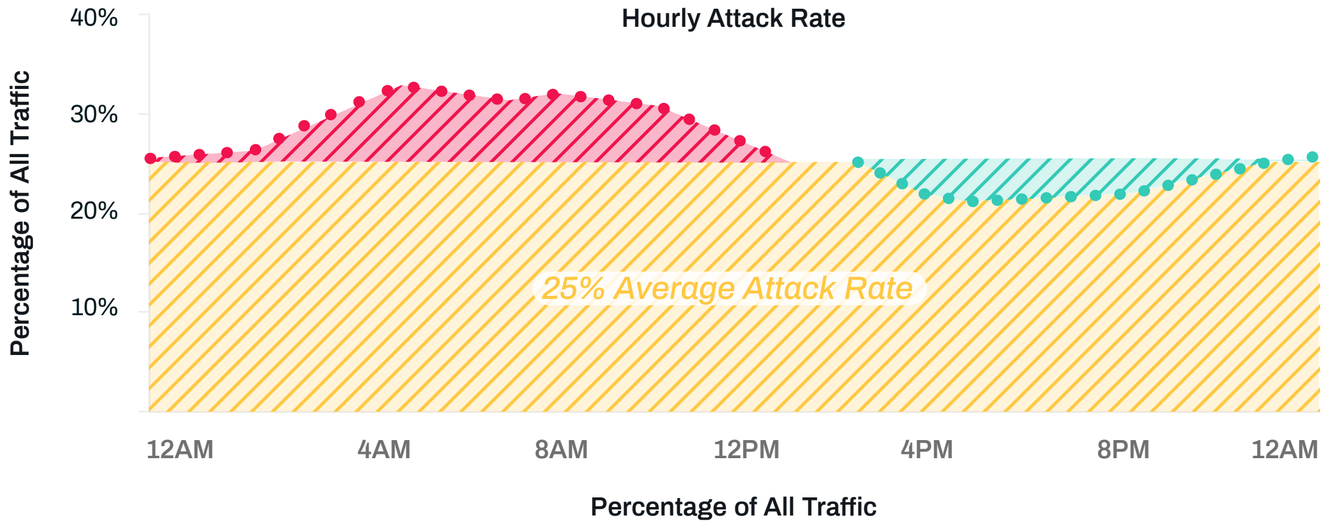






The Most Dangerous Hour of the Day

When comparing attack levels with legitimate traffic patterns, it is clear that the morning is most dangerous period of the day. Businesses are facing cross-border attacks from fraudsters operating across timezones and using automated scripts that can run through the night. Therefore, attacks do not always tie in with the peak hours of legitimate consumers. 5am is the time of the day that has the highest attack rate across all traffic, with attacks 10% higher than in the afternoon. Traffic coming between the hours of 4am and 10am is generally higher risk than other times during the day.



Highest attack rate at 5am

Elevated attack rates between 4am and 10am

Trend Spotting: Beyond Mitigation Focused Strategies

Gartner's Cool Vendor report this quarter flagged that in the current threat landscape, businesses need to go beyond mitigation-focused strategies that rely on threat scores and behavioral analysis. More robust fraud detection capabilities are required, in a way that still delivers great user experience. Arkose Labs' ability to combine risk assessments with targeted enforcement challenges in a user-friendly way, puts it in a unique position address this issue.

Arkose Labs was featured as a Gartner 2020 Cool Vendor in the report which highlights "interesting, new and innovative vendors, products and services" in the IAM and fraud space.

Gartner
COOL VENDOR 2020™

Cool Vendors in IAM and Fraud Detection

Highlights from the report:

"The balance between detecting and mitigating fraud and creating low-friction and seamless UX has never been as important."

The limitations of mitigation-focused strategies in defeating fraud and automated abuse.

Traditional CAPTCHAs are being beaten by automation.

Download the full report at arkoselabs.com/gartner

Report Methodology

The Q2 Arkose Labs Fraud and Abuse Report is based on actual user sessions and attack patterns that were analyzed by the Arkose Labs Fraud and Abuse Prevention Platform from January to June 2020. These sessions, spanning account registrations, logins and payments from financial services, ecommerce, travel, social media, gaming and entertainment were analyzed in real-time to provide insights into the evolving fraud and risk landscape.

Unsophisticated bot attacks don't result in a user session and thus have not been included in this report. The report focuses on attacks from fraud outlets that combine state-of-the-art technology with stolen identity credentials and human efforts.

The attack patterns have been analyzed across parameters and closely investigate the mechanics of inauthentic attacks as they range from automated bots to human 'sweatshop' driven attacks. These attacks focus on defrauding the businesses and their users through fraudulent account registrations, account takeovers or payments using stolen credentials.

Arkose Labs uses a bilateral approach that combines global telemetry with a patent-pending enforcement challenge to profile user activity in detail and act upon data in real time. This provides unique insights into attacker identification and classification, enabling the platform to deploy appropriate responses and countermeasures. Suspect sessions are identified when they show characteristics that have been classified as abusive or malicious by Arkose Labs, based on previous activity on other customers' digital properties.

While Arkose Labs supports multiple use cases across the customer journey, these have been broadly grouped under account registrations, logins and payments for the purposes of this report.

About Arkose Labs

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales: (800) 604-3319

Offices

San Francisco
250 Montgomery St 10th Floor, San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane, Queensland AU