NuData Security

mastercard

2021 REPORT

Consumer and Risk Trends

NuData analysts report on the latest findings

Contents

Foreword

Take care of your trusted users

Online traffic continued to rise in H2 2021 as consumers engaged in more digital activities, from event ticket purchases to bank transfers. That rise in traffic was accompanied by a rise in expectations. It is no secret that users increasingly demand streamlined, personalized online experiences, while remaining uncompromising on high security standards.

Protecting accounts and information is an important goal, especially when some industries — notably the event ticketing industry — saw triple-digit year-over-year growth in attacks in 2021. The positive news is that by focusing on improving the user experience, companies can also identify and mitigate attacks. In fact, companies should prioritize getting to know their good users so they can deliver better online experiences tailored to their unique needs. With the right tools, analyzing behavioral and device insights from good users makes bad actors easier and faster to spot — and stronger security follows.

To better understand these and other trends facing companies today, we collected and analyzed NuData insights from the Mastercard Trust Network in 2021. Among the millions of interactions we monitor and score daily, we delve into critical trends and recommendations including:

- **Good users should be your priority.** Since good users make up a majority of traffic across all industries, streamlining processes for them has an enormous impact. Look for ways to simplify online experiences and remove friction for good users, for example by eliminating unnecessary authentication steps.
- **Where users go, attackers follow.** As industries like event ticketing ramp back up in the wake of reduced pandemic restrictions, attackers are searching for fraud opportunities. And they're finding them. Attack volumes in event ticketing grew 170% year over year in 2021 — faster than the growth rate of legitimate traffic in the industry, at 126%.
- **Sophisticated attacks are now the default.** Sophisticated attacks, which imitate human behavior to thwart common bot detection tools, now form nearly half (47%) of attacks across industries. In the retail, event ticketing and streaming industries, a majority of attacks show signs of sophistication. Only finance and digital goods have a lower incidence of sophisticated attacks — 14% and 15% respectively.

By looking back at 2021, we can prepare for the challenges — and opportunities — of 2022 and beyond. We're excited to discover together what's in store.

Sincerely,

Michelle Hafner

Senior Vice President Product Strategy & Execution, NuData, a Mastercard company

Key global themes

User experience is king

As more consumers digitize their day-to-day lives, companies must cater to their desires for seamless, customized digital experiences. That means putting good users — who make up the majority of all companies' online traffic — first. This approach helps identify and mitigate risky traffic.

Attackers follow trusted users to sites and platforms

As legitimate traffic in the event ticketing industry rose last year, attacks ticked up close behind. Unfortunately, other industries show similar patterns. When legitimate traffic returns to a site, companies should be prepared to mitigate increased attacks as well.

Sophisticated attacks are still a threat

Attackers continue to adapt their tactics to fool standard bot detection tools, necessitating more advanced behavioral solutions from companies. For example, 40% of sophisticated attacks use clean IPs without prior association with suspicious activity, thwarting tools relying on reputational data alone.

Credential quality is down to pre-pandemic levels

Between H1 and H2 2021, the percentage of correct credentials used in attacks dropped from 9.9% to 1.7%, close to the pre-pandemic average of 1.4%. This decline was expected as newer internet users become more experienced online and adept at spotting phishing and other credential-stealing schemes.

Key numbers from 2021

170%

Increase in event ticketing attack traffic (2021 overall)

3/5

Industries saw a majority of sophisticated attacks* (2021 overall)

40%

Of sophisticated attacks use clean IP addresses (H2 2021)

58%

Year-over-year increase in online purchase traffic (2021 overall)

1.7%

Credential success rate (H2 2021)

**attacks that use scripting techniques to emulate human behavior.*

Global traffic trends by industry

Retail and eCommerce traffic

Holiday shopping gets an early start

In the second year of the pandemic, online retail traffic continued to grow significantly. While 2020 dramatically surpassed expectations for online growth, 2021 saw a further 24% year-over-year increase in overall traffic. Most of this growth took place in the second half of 2021, when traffic grew 51% over H1 2021.

This increase was likely aided by a longer than usual holiday shopping season. In 2020, NuData and Mastercard Spending Pulse™ reported the start of the online holiday shopping season as three weeks earlier than in previous years. In 2021, this trend continued with spikes in online purchasing starting even sooner, in the early fall.

Customers may have started their shopping earlier than usual in anticipation of supply chain issues and long shipping delays.

As we can see on the graph, 2021 saw an overall growth of online transactions in Q4 compared to the same period in 2020. Customers are also purchasing more online in general, even outside of seasonal peaks — 2021 saw a 58% year-over-year increase in online purchase traffic.

Risks and opportunities for retailers

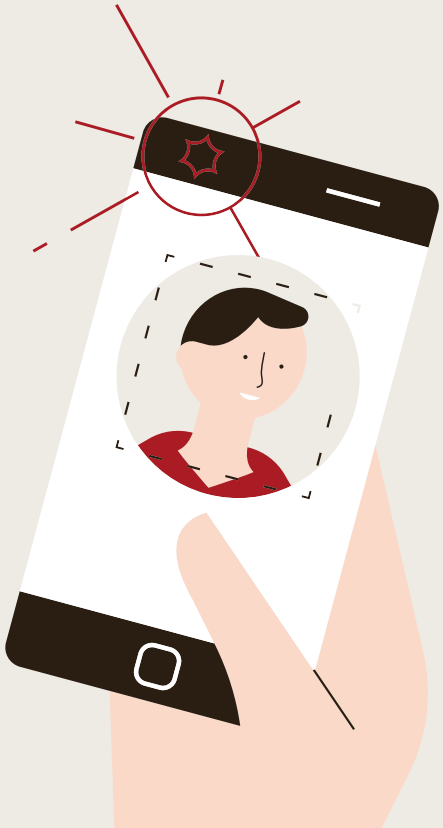
Though a growing online consumer base is good news for retailers, it comes with an unwelcome side effect. Overall eCommerce attack traffic grew 22% year-over-year in 2021. These attacks targeted multiple user journey touchpoints — including login, account update and checkout — but were intercepted by the NuData solution, NuDetect. Even with this rise in fraud, however, it's important for retailers to focus on improving experiences for trusted users, who made up 86% of all retail traffic in 2021.

22%

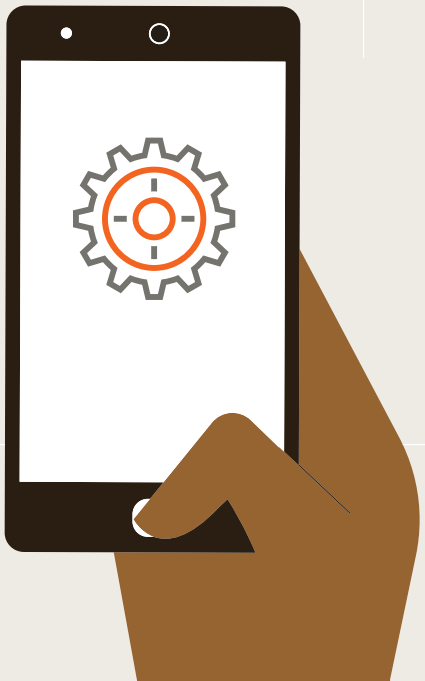
Growth in eCommerce attack traffic year-over-year in 2021

Targeted points of attack along a user journey touchpoints

Log-in



Account update



Checkout

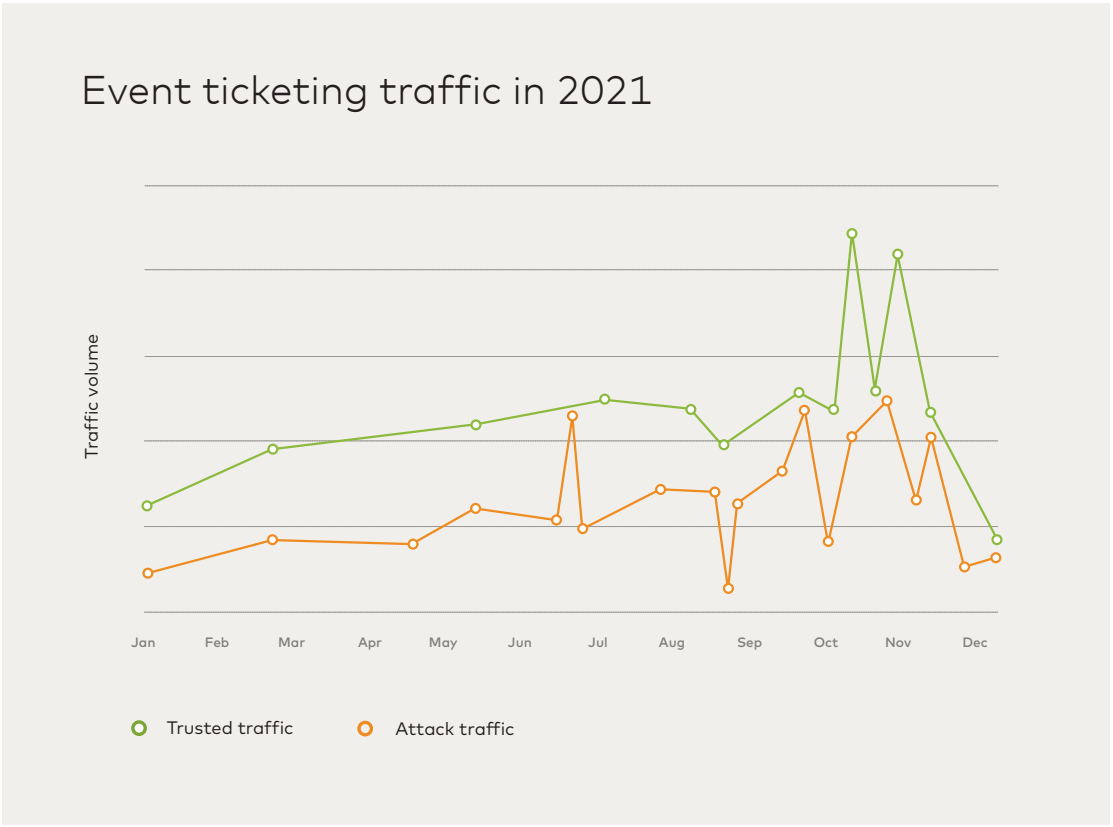
Event ticketing

The return of live events

The global event ticketing industry has seen a steady increase in traffic throughout the year, with a clear spike in Q4 as restrictions eased and holiday events ramped up. Overall, 2021 saw a 126% year-over-year increase in event ticketing traffic. However, traffic dropped at the very end of the year, most likely due to some countries enforcing new restrictions to slow the spread of the Omicron variant.

126%

Year-over-year increase in overall events traffic



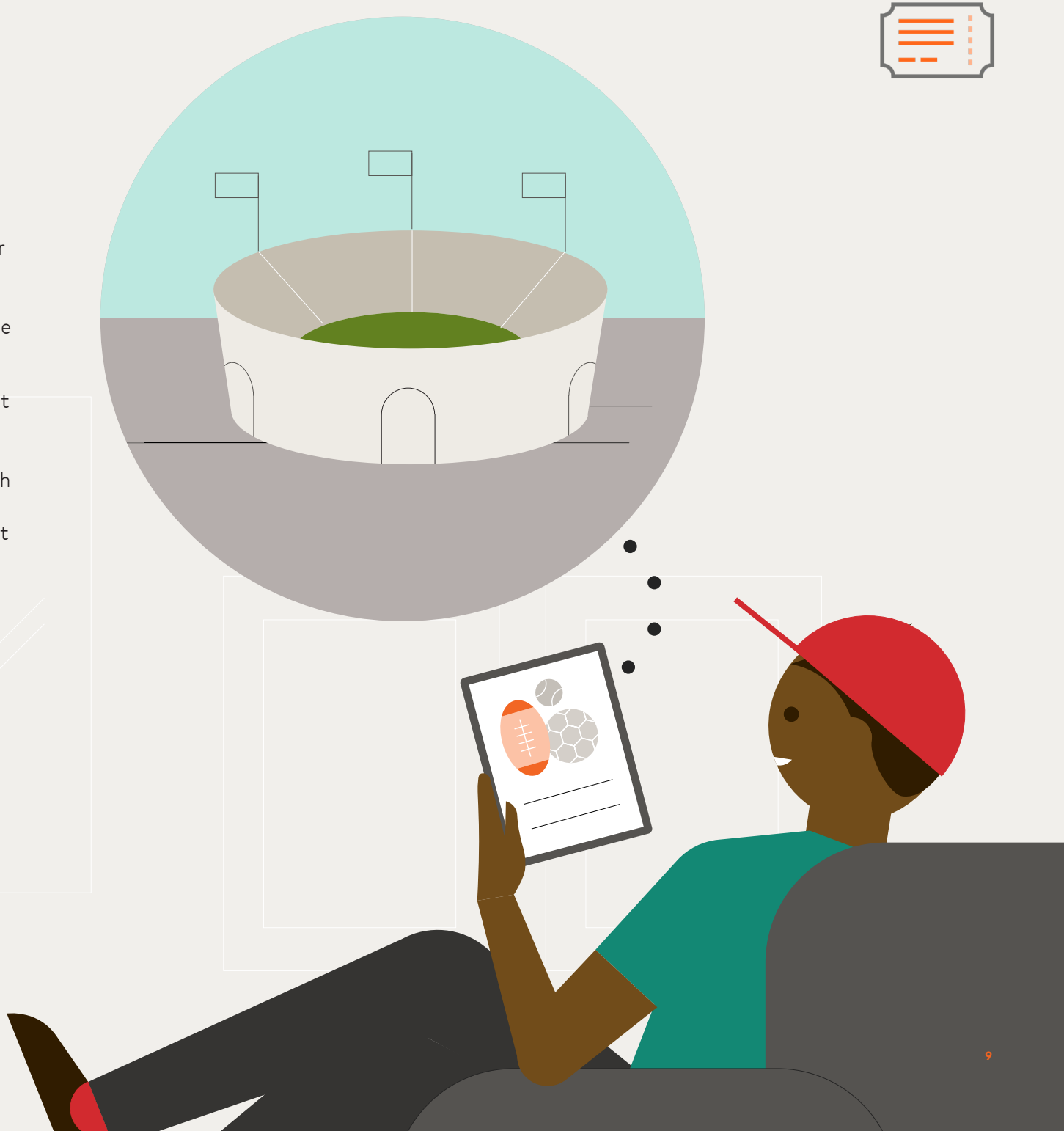
Risks to the event ticketing industry

It is suspected that attacks often follow the crowd, as bad actors try to hide within surges of trusted traffic. The second half of 2021 is a clear example of this pattern: As good users flocked to event platforms to buy tickets — particularly during November and December — attack volume rose accordingly.

In fact, attack traffic made up a third of all event ticketing traffic in 2021 (see graph on previous page). Rising 170% year-over-year, attack growth outpaced the rise in trusted traffic, which came in at 126% year over year. Though these threat increases are dramatic, they're a sign that some sense of normalcy has returned to our world. As more regions relax restrictions, customers are heading back to event ticketing platforms — and so are the attackers who left event ticketing to target other, more susceptible and active industries during the height of the pandemic.

170%

Year-over-year increase in attack traffic, which outpaced the rise in trusted traffic



Financial institutions

User experience should be a priority as online banking grows

Traffic from financial institutions (FIs) continued to show steady growth in 2021, with a 12% year-over-year increase. It's clear banking consumers are continuing to shift their business online. The number of banking users (measured as monthly accounts) rose 42% year-over-year in 2021, and total online fund transfers increased 54% year over year. At an individual level, users also interact with their accounts more frequently, with a 10.6% increase in interactions year-over-year.

In 2021, 85% of online traffic for FIs came from trusted users. As digital banking continues to grow, it's important for financial institutions to focus on improving experiences for trusted users, not just preventing instances of fraud. Consider that more than three-quarters (76%) of consumers are more likely to recommend a brand because it provides simpler experiences (World's Simplest Brands study, Siegel+Gale, December 2021). Simpler experiences are also tied to how users must prove who they are when engaging online according to Javelin Strategy & Research:

"The competitive landscape will also dramatically shift in favor of financial institutions that make it to market first with security options that consumers find convenient and appealing and that leverage biometrics, global device trust, and a variety of other parameters, such as geolocation and voice, as options for step-up authentication. Ultimately, the swiftest way for financial institutions to regain ground with consumers on issues of trust and ease of banking will be to layer technology that already exists with an arc of continuous authentication that is, in total, stronger than a static password alone." (2022 Financial Fraud Trends and Predictions, Javelin Strategy & Research, November 2021)

To streamline processes, financial companies should consider deploying online user validation solutions capable of building more accurate user profiles and offering convenient digital experiences. For example, verifying user identity through device intelligence and behavioral insights can enable the removal of cumbersome authentication steps, reducing friction for trusted users while keeping security standards high.

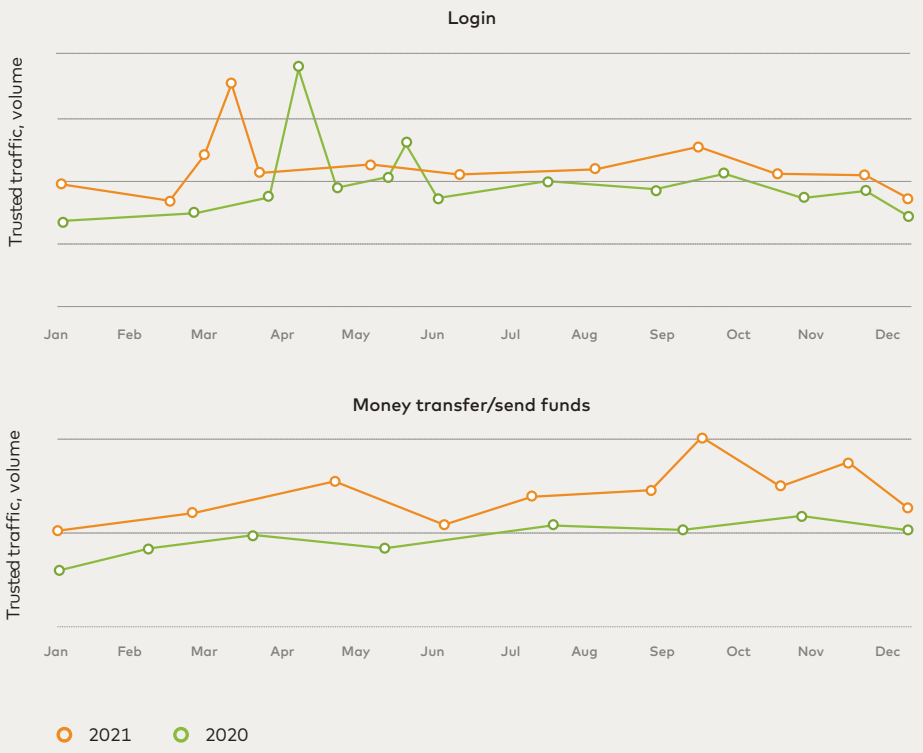
Risks to financial institutions

Attacks increased 15% from H1 2021 to H2 2021, which is slightly higher than the rate of growth of trusted traffic for FIs. The cost of fraudulent activity for financial institutions has also increased since before the pandemic. Between 2019 and 2021, the average cost of an instance of identity fraud rose by $256 to $1,551. (2022 Identity Fraud Study: The Virtual Battleground, Javelin Strategy & Research). By focusing on understanding the consumer's online behavior, it becomes easier to detect anomalies that compromise users' accounts.

15%

Increase in attacks from H1 to H2 in 2021

Financial institution traffic by user touchpoint, 2020 vs. 2021



A look at attack traffic

Sophisticated attacks across industries

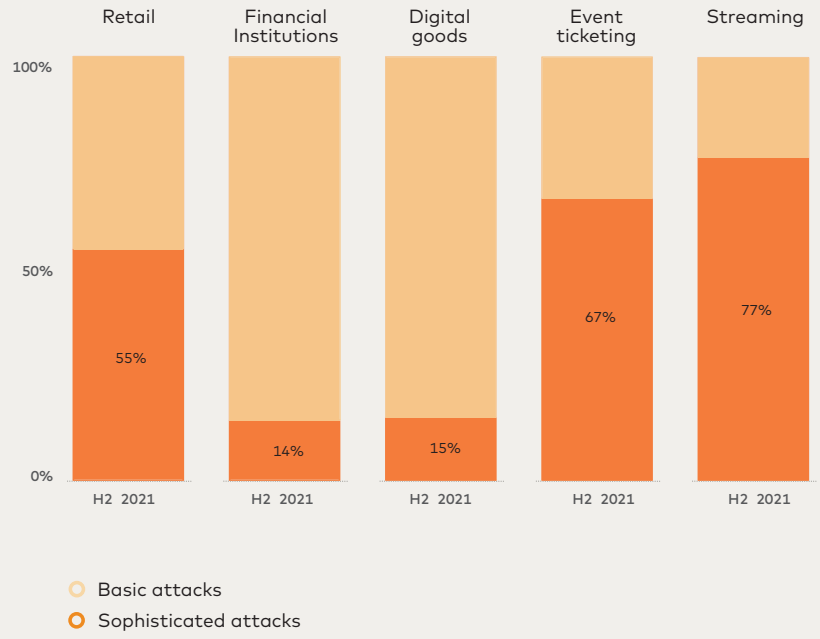
Sophisticated attacks imitate human patterns of behavior to evade common bot-detection tools. Fraudsters' tactics can include anything from automated scripts emulating human typing patterns to schemes employing workers at "human farms" to solve CAPTCHAs and pass bot challenges.

After rising throughout the pandemic, complex threats are now common across the different industries we monitor — in 2021, sophisticated attacks represented the majority of attacks in three industries (retail, event ticketing, and streaming). Overall, the average rate of sophisticated attacks across all industries is 47%.

47%

Of attacks across all industries were sophisticated in 2021

Sophisticated vs. basic attacks by industry



Sophisticated attack traits in H2 2021

An examination of the most common behaviors among sophisticated attacks across the NuData network in H2 2021 reveals why they're so difficult for traditional tools to mitigate. A third (33%) use non-scripted techniques such as automated cycling of inputs to appear human and avoid detection. Forty percent use clean IPs not previously linked to risky activities, making it harder for tools relying on reputational information alone to flag them.

Detecting sophisticated attacks with the trust network

Spanning a wide range of clients and industries, the global trust network NuData has access to was able to detect 60% of sophisticated attacks in H2 2021. NuData intercepted the remaining attacks through an array of advanced solutions, namely behavioral tools that are difficult for even the most sophisticated attackers to fool.

Most common patterns in sophisticated attacks in H2 2021

Non-scripted attacks: 33%

Clean IPs (not linked to past risk): 40%

Flagged by the trust network: 60%

Credential success rate

When a company is under attack, quickly mitigating the threat is the No.1 goal. However, understanding the information used in the attack is also a helpful indicator of the type of data cybercriminals have access to, and is an item NuData tracks as well. Such insights can, in turn, be useful for anticipating and preventing future attack patterns.

In our H1 2021 report, we described how the influx of newer, often less tech savvy internet users at the start of the pandemic gave attackers an opportunity to harvest large volumes of high-quality credentials via phishing schemes. This fueled a spike in the percentage of correct credentials used during login attack attempts (though NuData clients were still able to foil those attacks).

At the time, we predicted that attackers' window of opportunity would likely be short. We expected high credential success rates to level off as new users gained knowledge and confidence about how to spot scams and protect their data. As forecasted, in H2 2021 we have indeed seen a sharp decrease in the quality of the credentials used in attacks. Only 1.7% of credentials were correct in H2 2021, down from 9.9% in H1 2021. This value is more in line with the 1.4% average credential success rate we saw before the pandemic.

While this decrease is good news, it's important to note it does not neutralize the threat. One login attack can include hundreds of thousands to millions of attempts, so a 1.7% rate of correct credentials can still compromise 17,000 accounts in a single attack. Even a slight increase in 2022 would represent thousands more good users at risk from a single attack.

Conclusion: key takeaways for 2022 and beyond

1. **Online traffic is growing and so are users' demands.**

Users today expect seamless online experiences customized to their specific needs no matter the industry. Trusted users make up the majority of every company's traffic, and they deserve to have their needs met. In 2022 – and beyond – companies should make plans to streamline and simplify their processes to offer the trustworthy majority of online users the most excellent experience possible.

2. **Online banking and eCommerce growth is a UX opportunity.**

Users are making more online purchases and money transfers than ever before. Companies should embrace this shift as an opportunity to get to know their users better. By accessing device and behavioral insights, companies can learn more about their users' needs and build purchasing and money transfer experiences customized to them.

3. **Where online traffic goes, attacks follow.**

As activity returns to pandemic-affected industries like event ticketing, good users are flocking back to platforms — and attackers are close on their heels. Companies should be ready to welcome returning users, but also have tools in place to spot malicious traffic in the mix. When companies focus on understanding the behavioral patterns of good users, it's easier to spot the anomalous behavior of bad actors.

4. **Sophisticated attacks highlight the need to access device and behavioral insights.**

Attackers leverage sophisticated scripts and human workers to bypass security tools — and these types of attacks are increasingly the default across most industries. This means companies require behavioral tools that can do more than spot basic bot behavior, seeing through attacks craftily disguised as legitimate traffic.

Glossary of terms

Bot-detection challenge: When an event is suspected to be fraud, a bot-detection challenge such as a CAPTCHA helps confirm if it is a machine or a human.

Bot-detection tool: Tools detecting bot behavior by looking at some data such as IP, location, connection, or input.

Digital goods: Companies selling any goods that are stored, delivered and used in their electronic format, including SaaS.

eCommerce: Companies buying and selling goods or services online.

Event ticketing: Companies that sell tickets for online or in-person events such as concerts or conferences.

Financial institutions: Institutions that provide financial services such as banking and credit unions, including FinTech (Financial Technology).

High risk: Session or sessions (client interaction) with a high-risk score that exceeds a baseline of a safe interaction, based on the NuData platform's assessment.

Mastercard trust network: The Mastercard Trust Consortium collects cross-client insights to assign risk scores to online events in real time and improve the accuracy of each assessment.

Sophisticated attacks: Attacks deploying lower volume but attempting to emulate user behavior, in part by displaying expected browser or application behavior. They are highly organized, have significant resources at their disposal, and run scripts in the environment to simulate human interaction.

Streaming: Companies that sell services for online viewing.

Success rate: In the context of an attack, the success rate is not how successful the attack was but how many credentials were correct, despite the attack being blocked. The success rate is the number of login attempts (mitigated) with correct credentials for every 100 attempts.

Touchpoint: User interaction points, such as account creation, login, and checkout.

Trusted users/traffic: Users interacting with the online environment who show little or no risk signals.

About NuData, a Mastercard company

Read our success stories to learn how we've helped other companies

If you have questions, email us at hellonudata@mastercard.com

NuData Security, a Mastercard company, helps businesses validate good users without disruption and stop bad actors before they can cause damage. With over 20 billion risk assessments processed and 4.5 billion devices seen yearly, NuData harnesses the power of behavioral signals and device intelligence to verify users, stop account takeover, prevent new account fraud, and reduce good user friction in real time. NuData solutions are trusted by some of the world's largest brands to prevent fraud while offering a seamless customer experience.

About Mastercard SpendingPulse™

Mastercard SpendingPulse™ reports on national retail sales across all payment types in select markets around the world. The findings are based on aggregate sales activity in the Mastercard payments network, coupled with survey-based estimates for certain other payment forms, such as cash and check. As such, SpendingPulse™ insights do not in any way contain, reflect or relate to actual Mastercard operational or financial performance, or specific payment-card-issuer data.

3.4B

accounts protected yearly

20B

risk assessments yearly

4.5B

devices monitored yearly

NuData Security

mastercard