NuData Security

mastercard

JANUARY 1 - JUNE 30, 2021

H1 2021: Fraud Risk at a Glance

NuData analysts report on cybersecurity trends

Contents

Foreword

Adapting security to a hybrid world

As we entered a new phase of the pandemic, vaccines helped some regions bring a sense of normalcy. In the first half of 2021 as vaccination rates rose, so did the number of in-person events and reopened stores, restaurants, and offices. This new phase also ushered distinct digital trends.

Consumers made it clear that they didn't want to leave the convenience and seamlessness of online interactions behind. Online traffic continued to grow as consumers leaned into hybrid experiences that combine online and offline activities, like buy online and pickup in store (BOPIS).

At the same time, deceleration of new account creation across industries signaled a new level of digital maturity among consumers. Users have already created their accounts and now it's up to companies to engage them with frictionless experiences driven by a digital-first strategy.

In this report, we leverage intelligence collected from the global NuData network in H1 2021 to explore this new hybrid world. Among the millions of events we monitor and score daily, we found that attackers have responded to the evolution of this complex digital ecosystem by refining and specializing their attacks:

- **More sophisticated attacks:** Attacks that evade standard bot-detection tools by imitating human behavior are becoming more common. They now make up more than 50% of attack volume in two-thirds of the industries we studied.
- **More testing of stolen credentials:** A rise in phishing and other scams during the pandemic yielded a bumper crop of personal information for sale on the dark web. Card cycling — a method for testing the validity of stolen credentials — increased 54% as bad actors looked to verify the data they'd purchased.
- **Higher rates of correct credentials:** Fraudsters are also brainstorming creative ways to increase attack efficacy, for example by artificially increasing their credential success rates to evade rules-based security protections. Almost 10% of credentials used in attacks in H1 2021 were correct, up from only 1.9% in 2020.

The new digital landscape contains new threats and new opportunities. With more users accessing more goods and services online, companies can leverage behavioral data that can help them design more personalized, streamlined experiences. In particular, they can use these new insights to remove friction for good users while enabling more accurate fraud detection, countering sophisticated attacks and other threats.

Together, let's prepare for the challenges of 2021 and beyond.

Sincerely,

Michelle Hafner

Senior Vice President Product Strategy & Execution, NuData

Executive summary and key global themes

Hybrid experiences are on the rise across industries

Even as more consumers returned to in-person shopping, eCommerce purchase traffic grew 51% in H1 2021 compared to the same period in 2020, signaling the growing importance of seamlessly combining online and offline retail experiences. Traffic across our FIs also rose 16%, and money transfers rose 23%, reflecting users' desires to retain the convenience of online banking even as branches reopen.

Event ticketing traffic is on the uptick — but so are attacks

With major events like concerts and festivals back on the agenda, event ticketing companies saw their traffic more than double in H1 2021. Unfortunately, attack volume also increased 2.4x in the same period, and 59% of attacks were sophisticated. Events companies need to equip themselves with the right tools to mitigate these threats.

Sophisticated attacks are here to stay... and evolve

Sophisticated automated attacks made up the majority of attack volume in events, retail and eCommerce, streaming and travel. By emulating human behavior, these attacks can evade detection by standard security tools. As they become commonplace, companies will require more advanced protections to defend against them.

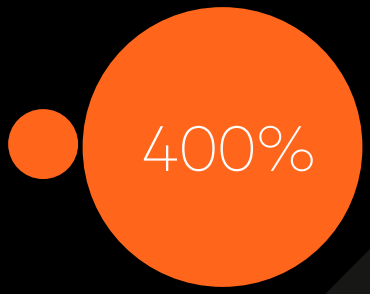
An influx of stolen credentials led to increased card cycling

As more activities moved online during the pandemic, scammers doubled down their efforts to trick users into revealing their personal information. The 54% uptick in card cycling — a method for testing the validity of stolen payment information — is a sign of these scams' success.

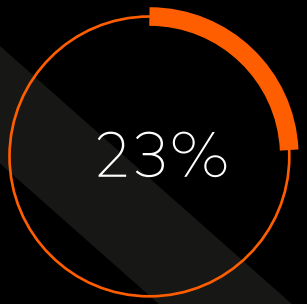
Attackers raised their credential success rates

The average percentage of valid credentials used in an attack spiked to 9.9%, up from 1.9% in 2020. This could be a sign that attackers have accessed high-quality credentials through phishing scams or data breaches — or a sign of sophisticated attacks that artificially boost credential success rates.

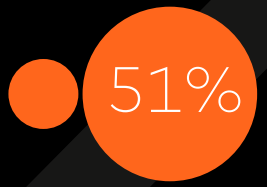
The first half of 2021 in numbers



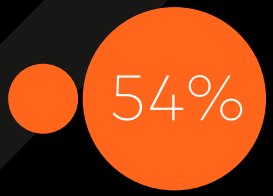
Traffic increase across event-ticketing companies, compared to 2020.



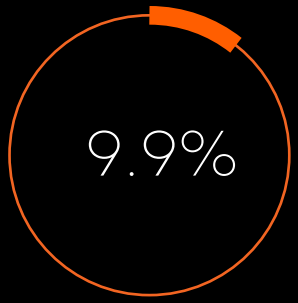
Increase in FI sophisticated automated attacks within H1 of 2021.



Growth in eCommerce purchases among major retailers, compared to H1 2020.



Year-over-year increase in card cycling attacks.



Correct credentials used in attacks during H1 of 2021, a new record.

Global traffic trends by industry

To understand how the easing of some pandemic restrictions impacted online activity, we examined traffic patterns across three of the largest industries on our network: retail and eCommerce, financial institutions, and event ticketing. The trends we identified highlight the growing importance of hybrid – blended online and offline – experiences as industries and users attain digital maturity, showing the need for companies to pursue a digital-first strategy to deliver seamless online experiences.

Retail and eCommerce

Financial Institutions

Event ticketing

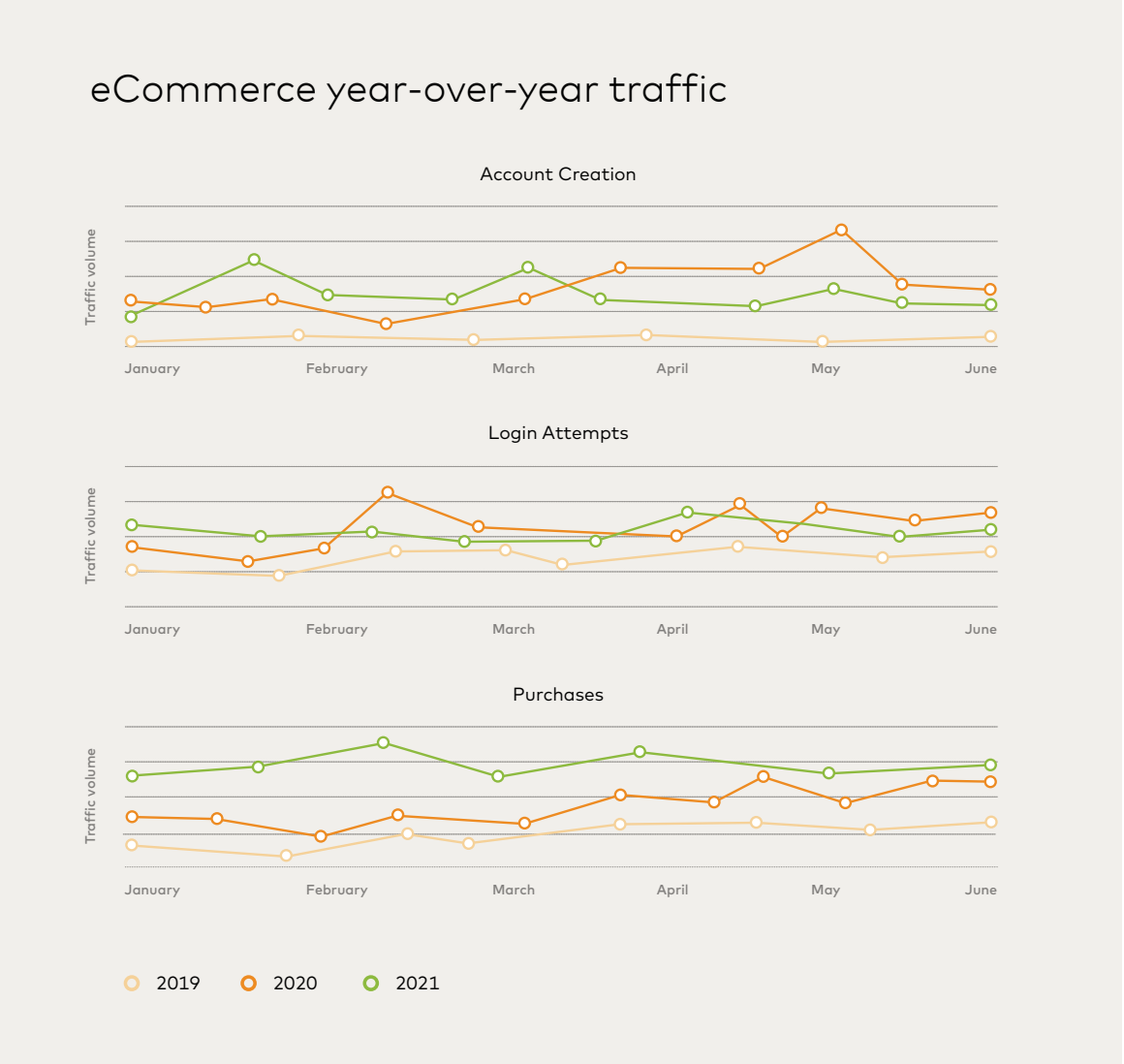
Retail and eCommerce traffic

A hybrid future sustains high eCommerce traffic

Hybrid retail experiences became the norm in H1 2021 as consumers realized the efficiency of blending eCommerce capabilities with in-person shopping. For example, after a dramatic spike in 2020, buy online, pickup in store (BOPIS) sales are still on the rise in 2021, and are expected to grow a further 15.2% year over year. Consumers are also taking advantage of many other hybrid retail capabilities, such as booking dining and travel plans via online portals and apps and loading online coupons onto their smartphones for use in-store.

These trends are reflected in continued strong eCommerce traffic in H1 2021, even after stores fully reopened in many regions. Online purchase traffic in particular has increased in H1 2021 compared to the same period in 2020. This corresponds to Mastercard SpendingPulse™ June findings in the U.S. that show eCommerce sales growing 8.3% year-over-year, reflecting an ongoing shift to digital.

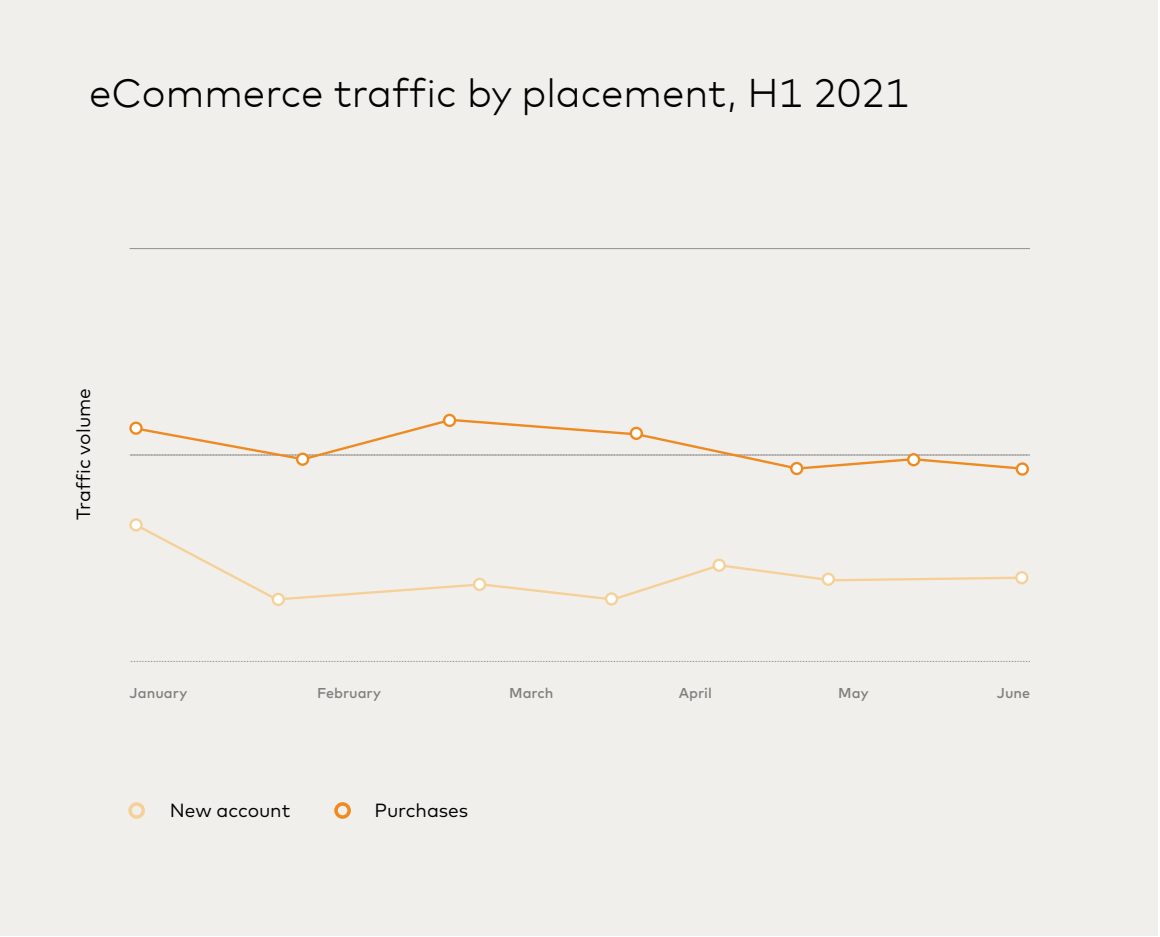
At the same time, consumers increased their physical purchases as restrictions eased, and ventured out more for meals. According to Mastercard SpendingPulse™ June insights from the U.S., consumers drove a 55.1% year-over-year increase in restaurant sales. They also went shopping both online and in stores to refresh their looks for summer camp, vacations, and travel, driving a 67.4% year-over-year sales increase for department stores and a 62.9% year-over-year sales increase for apparel merchants. All three categories saw more than 10% sales growth compared with 2019, showing that they've more than rebounded from the pandemic.



Online shopping reaches maturity

The volume of new eCommerce account opening requests monitored by NuData decreased by 15% from H2 2020, but that doesn't mean the digital revolution in retail is slowing down. It's important to consider the bigger picture: The volume of new account requests in 2020 and 2021 is still significantly higher than the volume in 2019 (see graph on page 8). There's been a sea of change in consumer shopping habits since the pandemic, and that means digital is here to stay.

The decrease in account opening volume in H1 2021 is actually a sign of digital consumer maturity. After a widespread transition to digital in 2020, much of the current eCommerce traffic comes from existing and returning users who don't need to open new accounts to shop. While many retail companies in our network have seen a deceleration in account openings, overall online traffic has remained strong. For example, purchase traffic in H1 2021 is 51% higher than the same period in 2020 among major retailers in our network (see graph on page 8), signaling that 2020's new users have become 2021's recurring customers.



51% **Increase in online purchases compared to same period in 2020**

Financial institutions

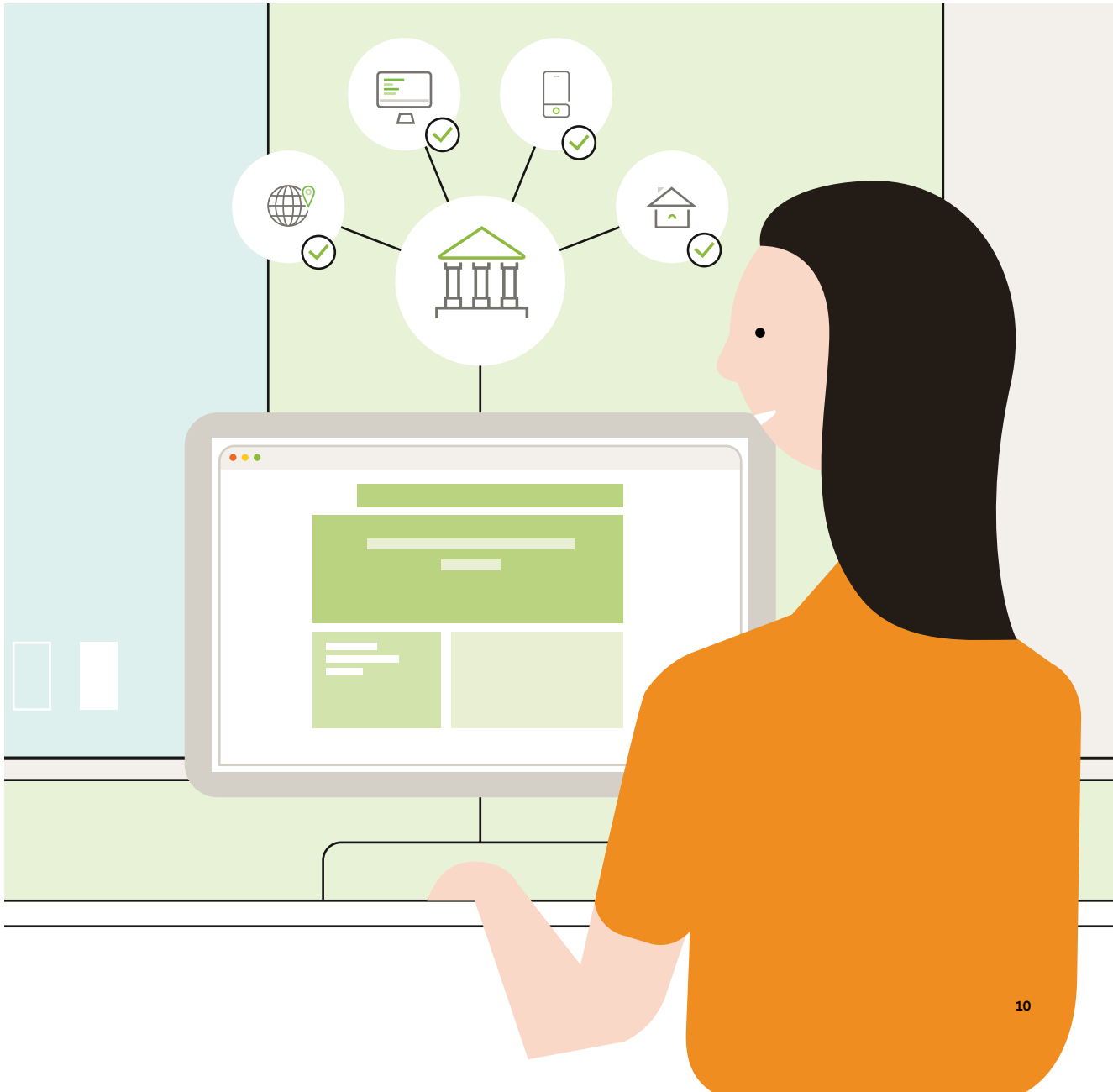
Unfrozen loans and reopenings drive finance traffic growth

As in eCommerce, the digital revolution in finance shows every sign of sticking. Even as branches reopened across multiple regions in H1 2021, online traffic in FIs held steady and even began to rise, increasing 16% over 2020. More notably, money transfers have increased 23% compared to H2 2020.

Part of the reason is simple: Now that customers have experienced the efficiency and convenience of online banking, few want to go back. According to research by Aite Group, at least 82% percent of consumers who used online or mobile banking for the first time plan to continue to use this delivery channel in the future.[1]

23%

Increase in online money transfers compared to H2 2020.

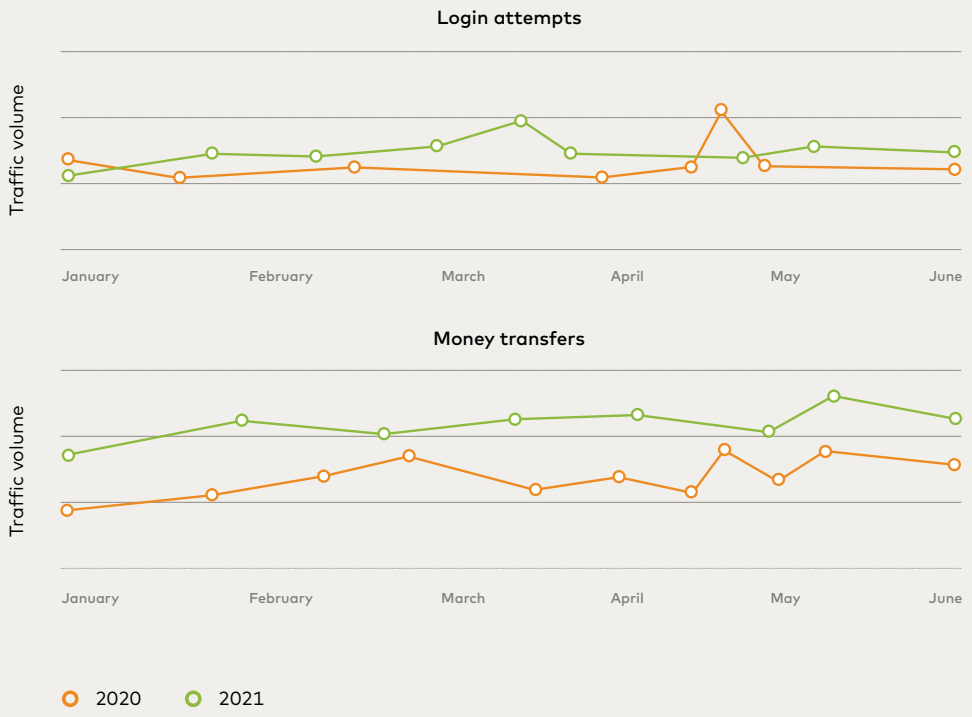


[1] *U.S. Identity Theft: The Stark Reality, Aite Group, 2021*

Uptake will continue to be strong even among vaccinated consumers who might feel comfortable returning to bank branches. In a recent IMC survey, two-thirds of vaccinated respondents said they see digital banking as a change that's here to stay.[2]

Another cause of increased traffic is customers' changing financial situations. Widespread reopenings of restaurants, stores, and offices made it possible for more people to return to work, enabling them to pay more expenses. At the same time, the loan assistance many financial institutions offered at the beginning of the pandemic began to expire, forcing users to resume monthly payments for everything from car loans to mortgages. According to the Consumer Finance Protection Bureau, the number of loans in assistance has been steadily decreasing since late spring 2020, after a spike in March 2020.

Financial traffic, year over year, H1 2021



[2] *Global Foresights, Insights & Analytics COVID-19 Consumer Impact Study, IMC, 2021*

Value of a digital-first strategy

With demand for online services showing no signs of subsiding, it's clear that financial companies need to have a strong digital presence to remain relevant and serve their customers' needs. The transition to digital isn't just a boon for customers — it's an opportunity for financial institutions, too. As more users interact online, companies have the opportunity to analyze new trends based on customers' habits, needs, and expectations. This data in turn can help companies build online services with experiences such as more streamlined authentication processes customized to the user.

At the same time, having more information and behavioral insight on good users can boost security, putting companies in a better position to detect anomalies and risky traffic. This is especially important as rates of identity theft continue to grow during the pandemic. Higher benefits and longer eligibility periods have made unemployment identity theft in particular more tempting to fraudsters, according to Aite Group.[3]

In addition, Javelin Strategy & Research found that the average identity fraud amount rose from $55 in 2019 to $1,350 in 2020, increasing financial services providers' losses per identity fraud incident.[4] Building behavioral insight is an important way for financial companies to protect both their data and their bottom lines.

[3] *U.S. Identity Theft: The Stark Reality, Aite Group, 2021*

[4] *The 2021 Identity Fraud Study, Javelin Strategy, 2021*

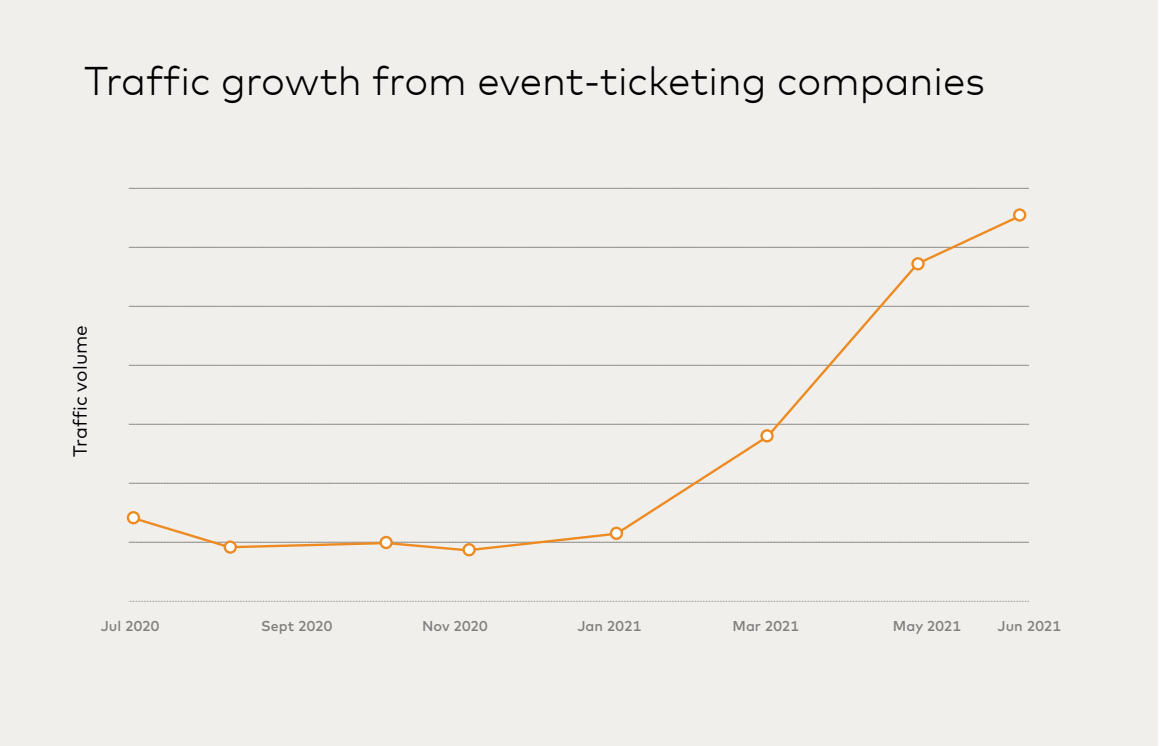
Event ticketing

Trusted traffic is on the rise

Overall traffic from trusted users has slowly increased for event-related companies as restrictions ease. From January to July 2021, we saw a rapid increase in traffic, reaching levels 400% higher than H2 2020. The trend has particularly accelerated since spring 2021, when many regions started easing restrictions more noticeably. We've all witnessed more in-person events being advertised and happening around our communities. Even with the resurgence of the Delta variant curtailing some gatherings, events are continuing to enjoy a comeback.

400%

Increase in events traffic compared to the avarage from H2 2020.

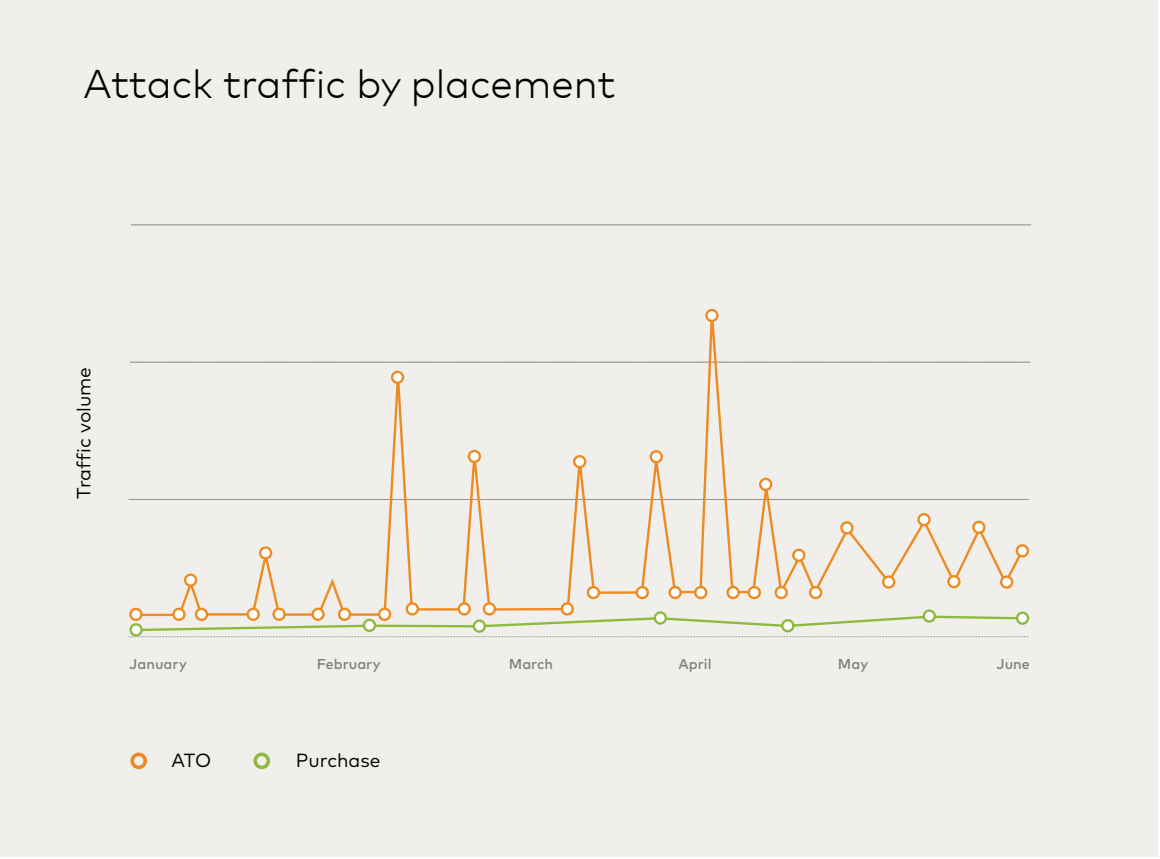


Unfortunately, attacks are also returning

As more in-person events returned, so did bad actors looking for lucrative ways to defraud the system. Online reselling of all sorts of goods has multiplied during the pandemic thanks to the wide availability of automated bots, known as scalpers, that can make purchases across multiple websites simultaneously.

This type of inventory fraud using scalper bots makes it harder for regular consumers to make ticket purchases and can be reputationally damaging for events companies.

In addition to scalping, the return of in-person events in H1 2021 has spurred a 2.4x increase in attack volume, including mass scripted credential stuffing attacks. While the first three months of the year just showed an occasional spike in malicious traffic (see graph on the right), by early May attacks became a constant flow. With these patterns in mind, it's important for events companies to put mitigation tools in place that can detect all types of automated activity, from account takeover attacks to mass purchasing by scalper bots.



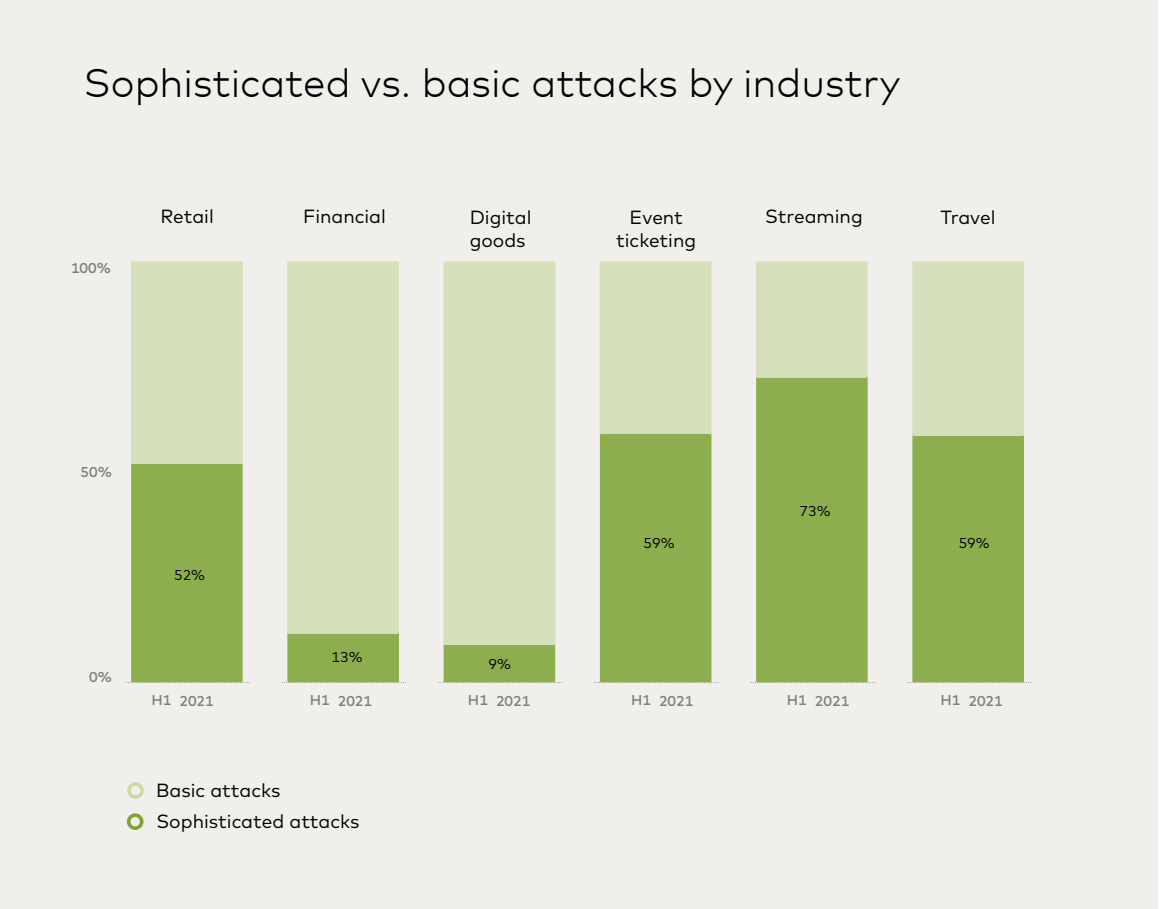
Global attack trends

Sophisticated attacks are here to stay... and evolve

Sophisticated attacks are here to stay

The expansion of sophisticated automated attacks, which emulate human behavior to evade detection, was a major concern in H1 2021. By imitating human keystrokes and mouse movements, among other behaviors, and even looping in human workers to solve CAPTCHAS or pass other security challenges, these bots can trick standard bot-detection tools through human workers. If a company doesn't have robust security protections in place, sophisticated attacks can do serious damage.

In 2019, sophisticated attacks first spiked in financial services before spreading to other verticals such as retail in 2020. Now, in H1 2021, they make up a majority of attacks in four out of the six industries where we examined these attack trends (digital goods, event ticketing, financial institutions, retail and eCommerce, streaming, and travel). In the event ticketing industry in particular, sophisticated attack growth was exponential, fueled by inventory fraud in which scalpers used bots to purchase large quantities of goods for resale. Unfortunately, the trend towards sophisticated attacks across all industries shows no signs of abating — but more innovative companies are improving their security, implementing behavioral tools to be prepared.



The rise of card cycling

In H1 2021, NuData noticed a trend at checkout across our eCommerce clients: a 54% year-over-year increase in card cycling. A type of credential stuffing attack, card cycling is a method for testing the validity of stolen payment information that involves making hundreds or thousands of small purchases using different payment information each time.

As the fraudster's automated bot "cycles" through their list of stolen credit card numbers or other data, it records which cards are declined and which are approved. At the end of the process, the fraudster has a list of valid credit card numbers they can use to make purchases themselves or resell on the black market for a high price.

Buyer beware on the black market

The spike in card cycling is a symptom of the overall increase in online financial fraud during the pandemic. With more consumers transacting online, scammers are finding creative ways to lure them into sharing personal information. Some tactics are highly technical, like overlay attacks that steal information by overlaying an invisible, transparent window over the touchscreen keyboard on a user's mobile device.

Others are more straightforward, like building a website for a fake retailer that takes customers' payment information, but never ships any goods. In the first months of the pandemic, Americans reported record-breaking numbers of undelivered online shopping purchases to the Federal Trade Commission — nearly double the number of reports received during the peak 2019 holiday shopping season. Many of the credit card numbers collected in these scams end up in the thriving online black market for stolen credentials, where they can be purchased by other fraudsters.

But in that market, it's buyer beware. Over time, consumers close email accounts, change passwords, and cancel credit cards, which means that much of the personal information for sale is outdated, if it was ever accurate to begin with. That's why so many fraudsters use card cycling to test the validity of credit card numbers before they use them in real purchases.

How to mitigate card cycling

Card cycling carries both monetary and reputational risks for companies. If a fraudster gets away with testing stolen payment information on your app or website, they're likely to try making a fraudulent purchase, too — leading to chargebacks and potential damage to your bottom line. Taking action to mitigate card cycling also avoids the brand damage that comes with having an insecure, poorly protected checkout.

If you have proper security protections in place on your eCommerce website or app, card cycling isn't hard to spot. Any user who inputs many different credit card numbers in rapid succession from the same IP address is likely a cycler. Looking at behavioral indicators like typing cadence can help identify automated activity, including card cycling scripts, too.

Improved credential quality during login attacks

As mentioned earlier, much of the stolen personal information used by fraudsters is outdated or inaccurate, forcing them to cycle through large numbers of credentials just to get a single hit. Historically, between 0.5% and 2% of login attack attempts across industries have used correct credentials. That might sound low, but when a single automated attack can input one million credentials, that 0.5%-2% of login attack attempts turn into thousands of compromised accounts and can do a lot of damage if other mitigations aren't in place to stop the attack.

In H1 2021, the average login credential success rate we observed on our network jumped dramatically to 9.9%, up from an average of 2% we saw in our network in 2020. The jump was particularly noticeable in the retail, streaming and event-ticketing industries, while finance remained the most stable.

While it's impossible to know exactly why credential quality has increased — particularly, why it increased so significantly in a handful of industries — four factors may play into the change.

	Digital goods	Retail	Financial	Travel	Streaming	Event ticketing
Successful credentials H2 2020	0.02%	1.18%	0.40%	1.37%	0.19%	3.95%
Successful credentials H1 2021	0.03%	12%	0.40%	1.7%	29%	16%

1. As-yet-undiscovered data breaches

It takes an average of 287 days before a data breach is discovered and contained, according to IBM.[5] A high credential success rate in a given industry could be a sign that a company in that industry has suffered a breach that simply hasn't been identified yet, resulting in the compromise of a large amount of personal information.

2. Attackers prioritizing rapidly-evolving industries

The transition to digital during the pandemic was incredibly fast and left many merchants handling large amounts of online customer data without much experience in how to secure it. Fraudsters aware of this may be targeting industries that began evolving digitally in the past 18 months, since they may be perceived as less experienced with fraud and security controls.

3. An increase in phishing

Fraudsters are acquiring valid credentials through phishing scams, which exploded in popularity during the pandemic. In 2020, Google registered a record 2 million phishing websites, an almost 20% increase over 2019.

4. Fake accounts created as part of sophisticated attacks

Many rules-based security tools automatically flag users with low credential success rates as potential bots. To evade detection, some attackers artificially improve their credential success rates by creating fake accounts (more in the case study in the next page).

[5] *2021 Cost of a Data Breach Report, IBM*

Case study: Artificially increasing credential success rate

2%

Average rate of success, until recently, for a credential stuffing attack.

70-90%

Success rate of legitimate users logging into their accounts.

40%

Rate of success recently discovered in a credential stuffing attack on our network.

As we mentioned earlier, until recently, it was rare for a fraudster carrying out a credential stuffing attack to see more than a 2% credential success rate. So, if even 5% of the credentials they used turned out to be valid, they'd likely be celebrating a resounding success.

At NuData, we know that when an attack appears to contain a high percentage of correct credentials, it doesn't necessarily mean the attacker had a good quality dataset. So, when we encountered an attack with an unheard-of 40% credential success rate on our network, even if we mitigated it, we decided to look at ways they might have gotten so many credentials right.

This attack included tens of thousands of login attempts. However, we quickly realized it didn't originate at login, but at account creation — a placement that the client was protecting with a non-behavioral solution. The attacker was able to achieve a high credential success rate in part because many of the accounts they were logging into, they created themselves.

If this sounds pointless, it isn't — because the rate of correct credentials in an attack can impact the deployment of the attack itself.

Remember, the average credential success rate of an automated attack at login is usually low — less than 2%. By contrast, legitimate users only mistype their passwords occasionally, giving them success rates in the 70% to 90% range. That's why some companies protect their login pages with simple rules that identify any user with a high number of failed logins as a potential bad actor. By artificially raising the credential success rate, an attacker can get around these rules and improve their chances of succeeding in the attack.

4 ways fraudsters artificially raise the credential success rate

1

Purge data

Before attempting to log in, the attacker runs their list of stolen usernames at the new account or password reset placement to check if these usernames exist. When they try to open an account with an existing username, the platform will return an error saying the account already exists. Now the attacker can rule out any nonexistent usernames on their list before starting the attack at login, lowering the failed-login rate.

2

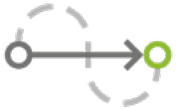
Create new accounts

To increase the credential success rate further, the attacker creates new accounts en masse with usernames and passwords they know.

3

Test at login

Attackers now finally deploy the attack at login, combining login attempts on their own accounts with login attempts on those stolen accounts they are targeting. They don't know the passwords for the targeted accounts, but know the usernames exist and have a set of username and password combinations to test.



4

Reap the benefits

By removing credential sets from usernames that don't exist in that platform and by including their own accounts in the attack, they can reach a high enough credential success rate to fool many rules-based security tools. In this case, they reached a 40% correct-credential rate.

Results

Fortunately, the login placement was protected by more than just a few simple security rules. NuData's solution detected and mitigated these tens of thousands of login attempts at a +99% rate, protecting the accounts and the subsequent direct fraud losses, brand damage, and customer churn. NuData's NuDetect solution did this by leveraging behavioral biometrics and analytics to flag anomalous activity. In particular, a few behavioral red flags showed us that the person making these login attempts with stolen credentials was unlikely to be the true owner of any of the accounts:

- Anomalous typing behavior at login compared to expected user behavior
- Unusual device information compared to expected user
- Anomalous bot behavior solving a challenge compared to the general population

+99%

Rate of detecting and mitigating these attcks using NuData's solution

Conclusion: what the data tells us about the future

1.

Hybrid experiences are here to stay: Even as pandemic restrictions ease, demand for online experiences isn't going away — in fact, many industries are approaching digital maturity as they reach a critical mass of returning online customers. As consumers continue to transact online and lean into hybrid services like BOPIS, companies must prioritize building out digital-first strategies that deliver seamless, friction-free experiences while still maintaining security.

2.

Exposed credentials make attacks more dangerous: Companies are still feeling the impact of the surge in phishing and other forms of fraud during the pandemic. The high numbers of credentials stolen in those schemes may have helped raise credential success rates to record highs, as well as fueling an increase in card cycling. These trends are likely to continue through the rest of 2021, making it even more important for organizations to build robust security protections that will mitigate these attacks, even if they present the right credentials.

3.

Need to build customized user experiences: The transition to digital experiences opens up new realms of possibilities that companies should take advantage of in 2021 and beyond. With more activities taking place online than ever before, companies can leverage behavioral information that can be used to personalize experiences for their customers — and build stronger security protections. By getting to know their good users better, companies can learn to flag bad actors faster and more accurately, resulting in a positive user experience that's more secure and nearly friction-free.

Glossary of terms

Account creation or online account origination fraud: The opening of a new account with fake or stolen information with the intent of committing fraud.

Account takeover: A fraudster illegally accesses a victim's account for fraudulent purposes.

Basic attacks: Attacks focused on quantity rather than quality. They don't attempt to emulate human behavior or browser interaction, and they typically don't execute JavaScript. They are characterized by displaying high velocity and cloud-hosted IPs.

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

Hybrid user experience: A user journey that combines online and offline actions, such as purchasing online and picking up in store.

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.

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

Sophisticated attacks: Attacks deploying lower volume but attempting to emulate user behavior. They display 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.

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.

Trust Consortium: Historical data of events and accounts aggregated from the NuData network to improve the accuracy of each assessment. NuData hosts the largest behavioral network, with 650 billion behavioral events monitored only in 2019. This data is hashed and doesn't include personally identifiable information.

About NuData, a Mastercard company

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

If you have questions, email us at verifygoodusers@nudatasecurity.com

NuData Security is a Mastercard company. It helps businesses identify users based on their online interactions and stops all forms of automated fraud. By assessing over 1.7 billion behavioral events each month, NuData harnesses the power of behavioral analytics and passive biometrics, enabling its clients to distinguish legitimate users from high-risk ones. This allows clients to verify users before a critical decision, block account takeover, stop automated attacks, and reduce customer insult. NuData's solutions are used by some of the biggest brands in the world to prevent fraud while offering a great customer experience.

+100M

accounts protected monthly

99.9%

risk-mitigation accuracy

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.

Mastercard SpendingPulse™ defines "U.S. retail sales" as sales at retailers and food services merchants of all sizes. Sales activity within the services sector (for example, travel services such as airlines and lodging) are not included.

NuData Security

mastercard