NuData Security
mastercard

JANUARY 1 - JUNE 30, 2020

2020 H1: Fraud Risk at a Glance

NuData analysts report on cybersecurity trends

Contents

Foreword

Human-looking attacks are here to stay

The COVID-19 pandemic has seen the fastest transition of customers moving to the online space and witnessed an unprecedented surge in the creativity of credential-stealing scams.

Now, online companies adapting their business models to enhance online servicing have to grapple with growing customer needs and more human-looking attacks. This report, based on NuData intelligence, highlights the changes in user habits and online threats, and helps companies prepare for the remainder of challenges and opportunities in 2020 – and beyond.

From January 1 to June 30, NuData analysts closely monitored global online changes across the NuData network, and summarized the key findings to help make sense of what's happening in the threat landscape.

Human-looking or sophisticated attacks, those that focus on quality instead of volume, continue to increase. Over the last six months, NuData found that almost all attacks against financial institutions were sophisticated attacks. These are high-quality attacks that try to resemble human behavior and often include human intervention, for example, to solve a CAPTCHA manually. This sophistication allows them to bypass common security layers, such as bot detection tools. Behavioral solutions like NuData's NuDetect, that monitor inherent user interactions, are more important than ever to identify the nuances of fraudulent attacks.

This analysis is enriched by the NuData Trust Consortium, a powerful host of information about attempted attacks on NuData clients. The Consortium is used to gather historical trends and train the machine learning models for attacker recognition and fraud prevention solutions. The insights developed by the Trust Consortium inform Mastercard's approach to protecting trust and securing the entire digital ecosystem.

If you would like to get more information on fraud trends, please reach out. We love talking about fraud – and of course, how to prevent it.

Sincerely,

NuData Analyst Team
verifygoodusers@nudatasecurity.com

The first half of 2020 in numbers

96%

Of attacks on FIs were sophisticated

124%

Growth in the average dollar value of a chargeback

55%

Growth in high-risk mobile traffic

360%

Increase in travel traffic since pandemic lockdown

More attacks look like humans

96% of login attacks on financial institutions were sophisticated – those that make an extra effort to emulate human behavior.

Account creation attacks increased as people stayed home during the pandemic

High-risk account creation attempts among a number of merchants increased after the lockdowns began.

Chargeback dollar values more than doubled

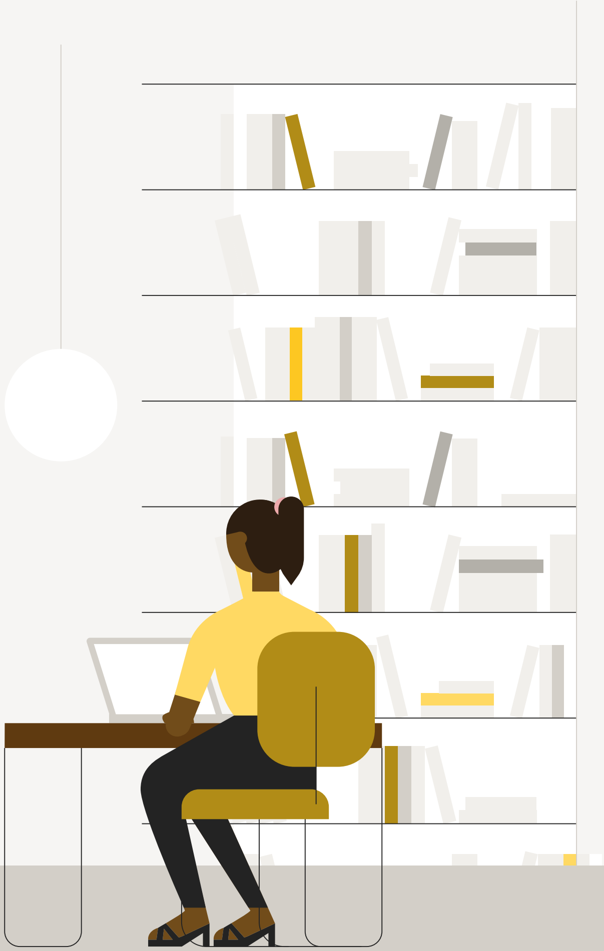
In North America, once the lockdowns were in place, the average dollar value of a chargeback grew by 124% for in-store pickup (chargebacks issued for various reasons after the goods were picked up), compared to the average dollar value before the movement restrictions.

Attacks leveraged the mobile channel

Mobile high-risk traffic grew 55%.

Travel-related traffic started coming back as communities opened

After traffic volumes hit their lowest levels in April due to the pandemic, the travel industry has started to recover, with a 360% increase in traffic since April.



Attacks are becoming more sophisticated - what does that mean?

Common mass-scale attacks, known as basic attacks, allow bad actors to test a higher number of credentials against a platform in very little time.

However, these basic attacks often show high velocity, or make use of the same IP addresses, making them easy to identify by bot detection tools. When bad actors see their basic attacks are caught, they evolve their attacks to hide bot telltales.

The wave of attacks with scripts that mimic human behavior – known as sophisticated attacks – are generalized across industries. Bad actors continue their shift to more complex schemes, attempting to fool security tools that can only detect basic bot behavior.

For the purposes of this report, basic and sophisticated automated attacks are defined as follows:

A **basic attack** focuses on high volume rather than quality. It doesn't attempt to emulate human behavior or browser interaction and it typically connects directly with the server, without executing JavaScript.

A **sophisticated attack** may show lower volume but attempts to emulate user behavior, increasing its effectiveness. It displays expected browser or application behavior and runs scripts in the environment to create this human-like interaction.

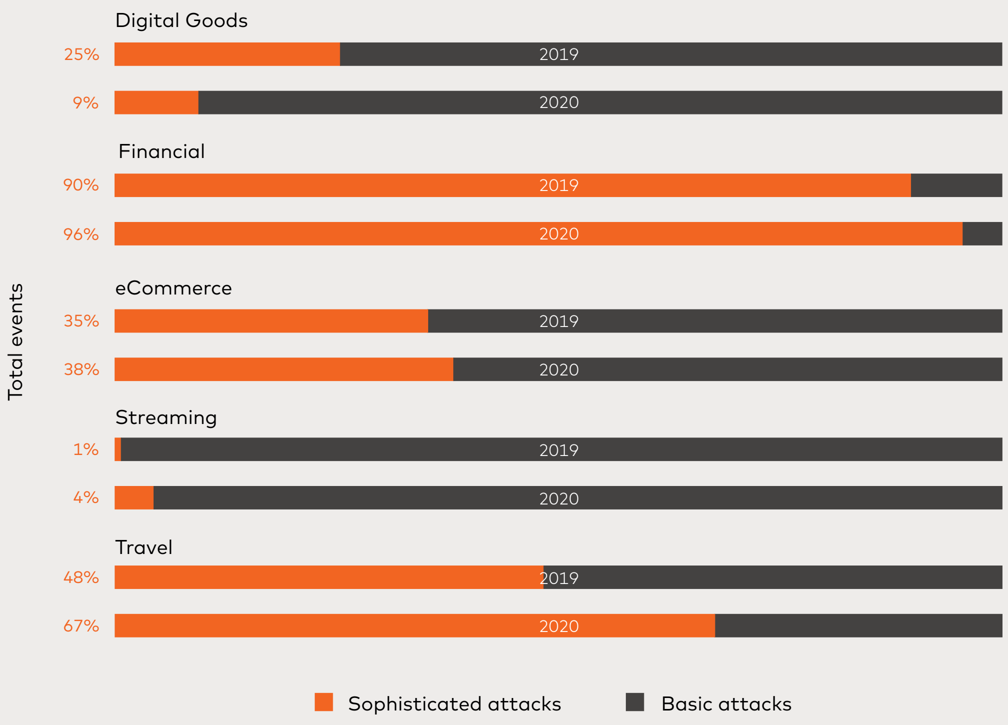
Sophisticated attacks on FIs

Financial institutions (FIs) receive the highest percentage of sophisticated attacks amongst all industries, with 96%, up from 90% in 2019.

After grappling with basic attacks for some time, FIs have steadily improved their security tools to detect and mitigate basic, volume-focused attacks. As a result, bad actors who know their basic attacks won't work against FIs, are forced to use more sophisticated attacks that could bypass bot-detection security tools. Similarly, as bad actors see their basic scripts fail against financial institutions, they move those attacks to other industries where they may be more successful. It's a clear case of recycling attack vectors across industries before working on improving them.

We expect to continue seeing human-looking attacks increase across all industries. As companies get wise to fraudsters and improve their bot-detection tools, fraudsters are forced to find another way in and rely more on sophisticated attacks to help them access protected platforms.

Sophisticated vs. basic attacks by industry

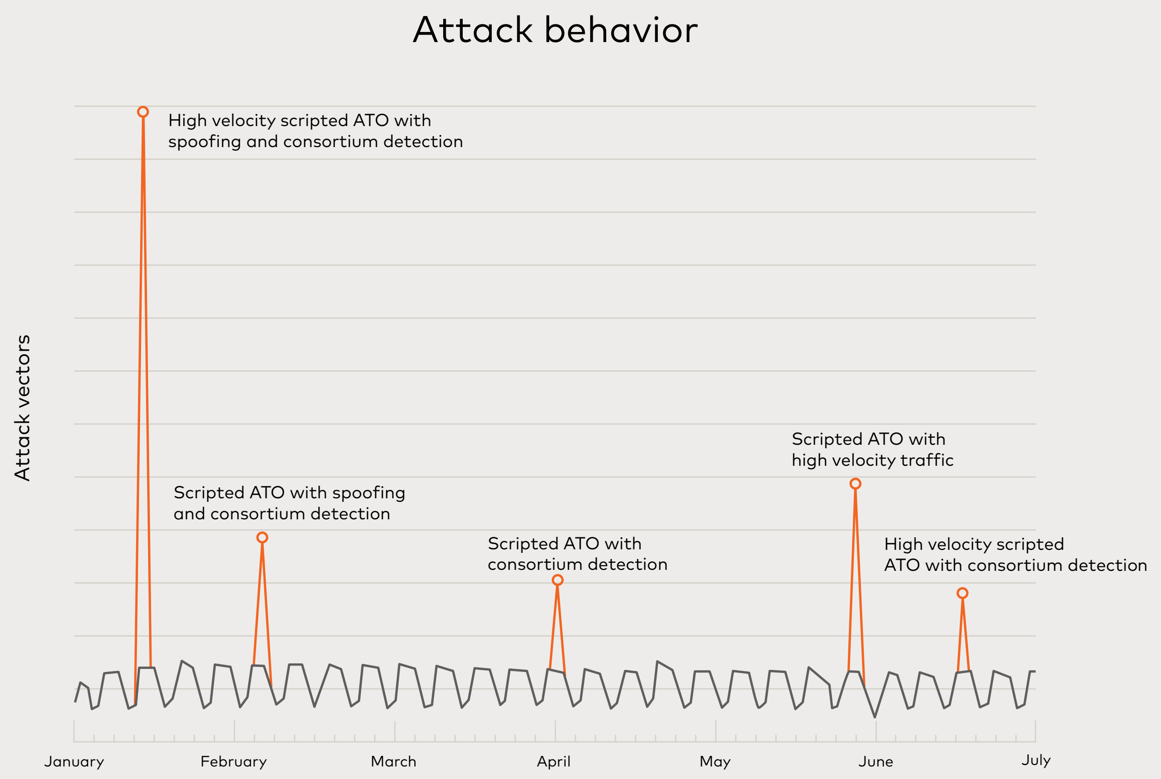


Source: NuData, 2020

Attack behavior

Each attack vector has its own characteristics, but they share common traits.

The graph beside shows a selection of account takeover attacks and their most identifying parameters. These attacks are discovered either by their high velocity or flagged through NuData's Trust Consortium. This ability to cross-check data, like IP and device identifiers with the Trust Consortium, helps companies detect attacks even if they are from a seemingly first-time user.



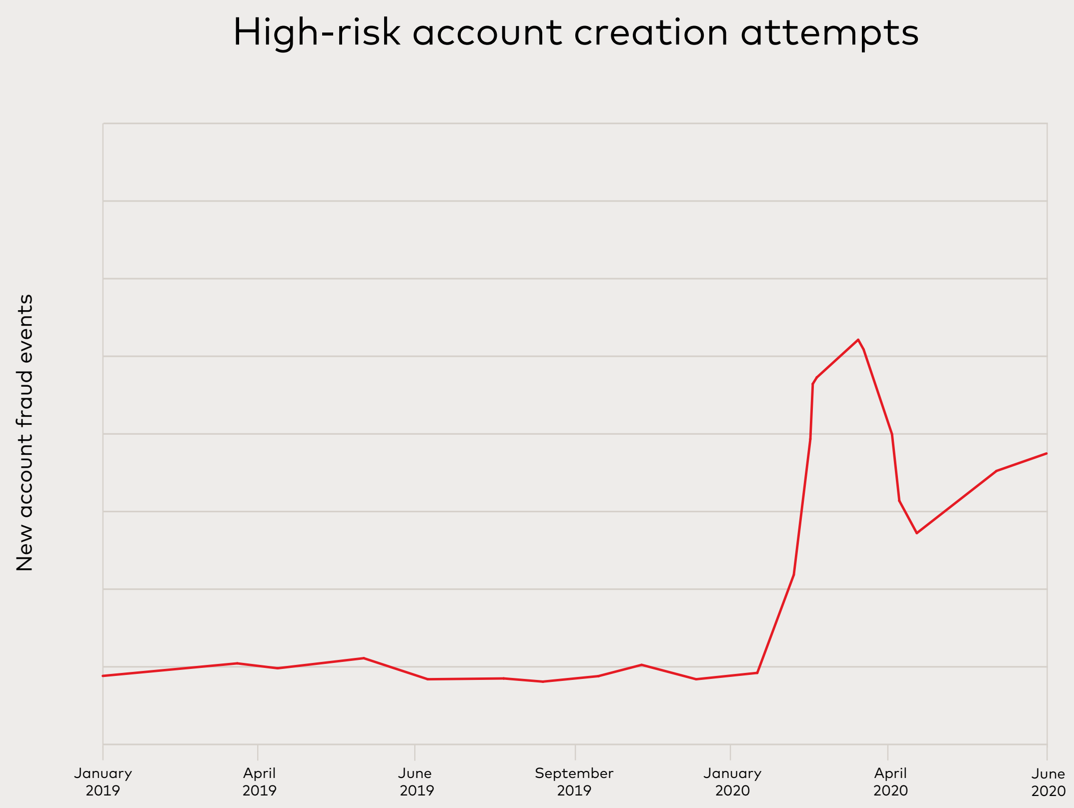
Source: NuData, 2020

Growth of new account fraud

Account creation attacks against a number of merchants, where bad actors create fake accounts for subsequent fraudulent use, have increased during the pandemic, compared to the same period in 2019.

The growth in this type of attack is influenced by bad actors using new accounts to make fraudulent purchases with stolen card information or to buy sought-after and restricted goods at mass scale for later resale. In particular, from March to June, one in every two account creation attempts was flagged as high risk by the NuData platform.

Fraudulent new accounts in the eCommerce space are also a step for illegitimate actions such as writing fake reviews, triggering video plays and likes, abusing sign-up offers, or hoarding items at checkout.



Source: NuData, selection of eCommerce companies ,2020

Pandemic traffic by industry

"In general, traffic hasn't gone down as much as it has shifted from one industry to another after users have seen their needs change."

Randy Lukashuk, CTO, NuData

The pandemic has affected online traffic differently based on the industry. NuData analysts have reviewed the changes in traffic across the largest industries in our network: retail or eCommerce, digital goods, financial institutions, travel, and ticketing companies. In general, as Randy Lukashuk, NuData CTO, pointed out, "traffic hasn't gone down as much as it has shifted from one industry to another, after users have seen their needs change."

The next pages analyze the changes to traffic volume globally across industries.

Events

Digital Goods

eCommerce

Financial Institutions

Travel

eCommerce and digital goods

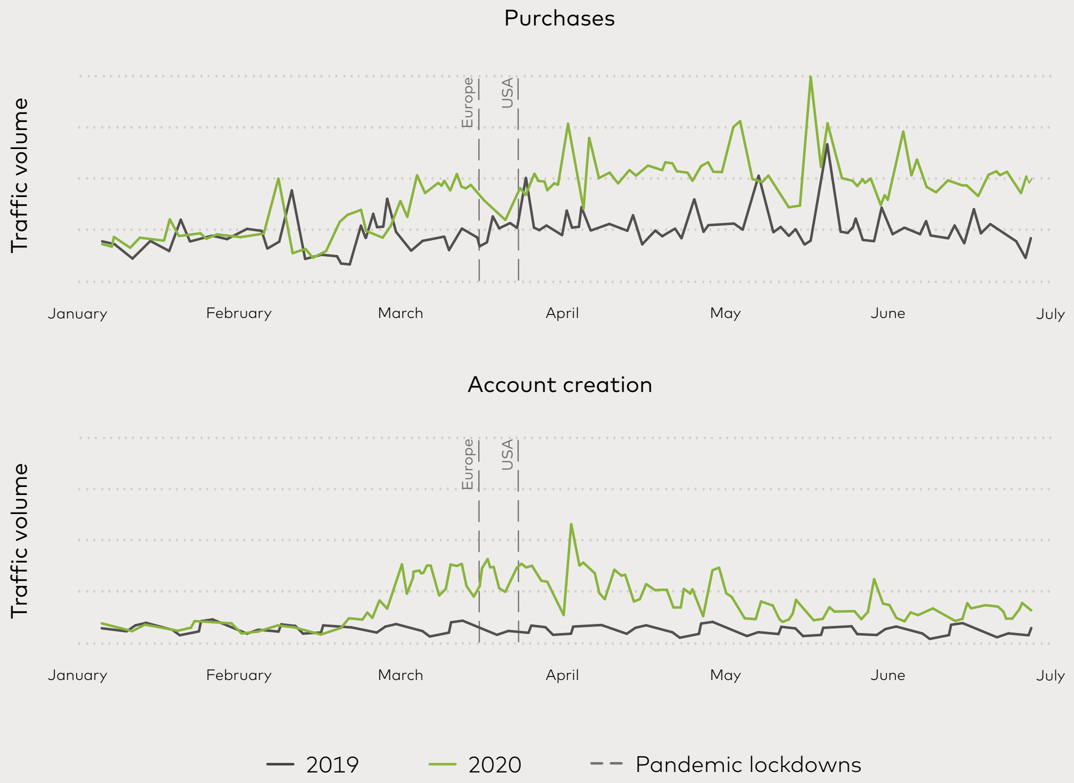
As the first lockdowns came into effect at the beginning of March and people made more purchases from home, eCommerce and digital goods traffic started to increase.

These graphs show traffic volume changes between 2019 and 2020, divided into account creation and checkout (two common user interaction points). Overall, eCommerce and digital goods companies had an average traffic increase of 67% compared to 2019.

67%

Increase in eCommerce and digital goods traffic from 2019

eCommerce traffic globally

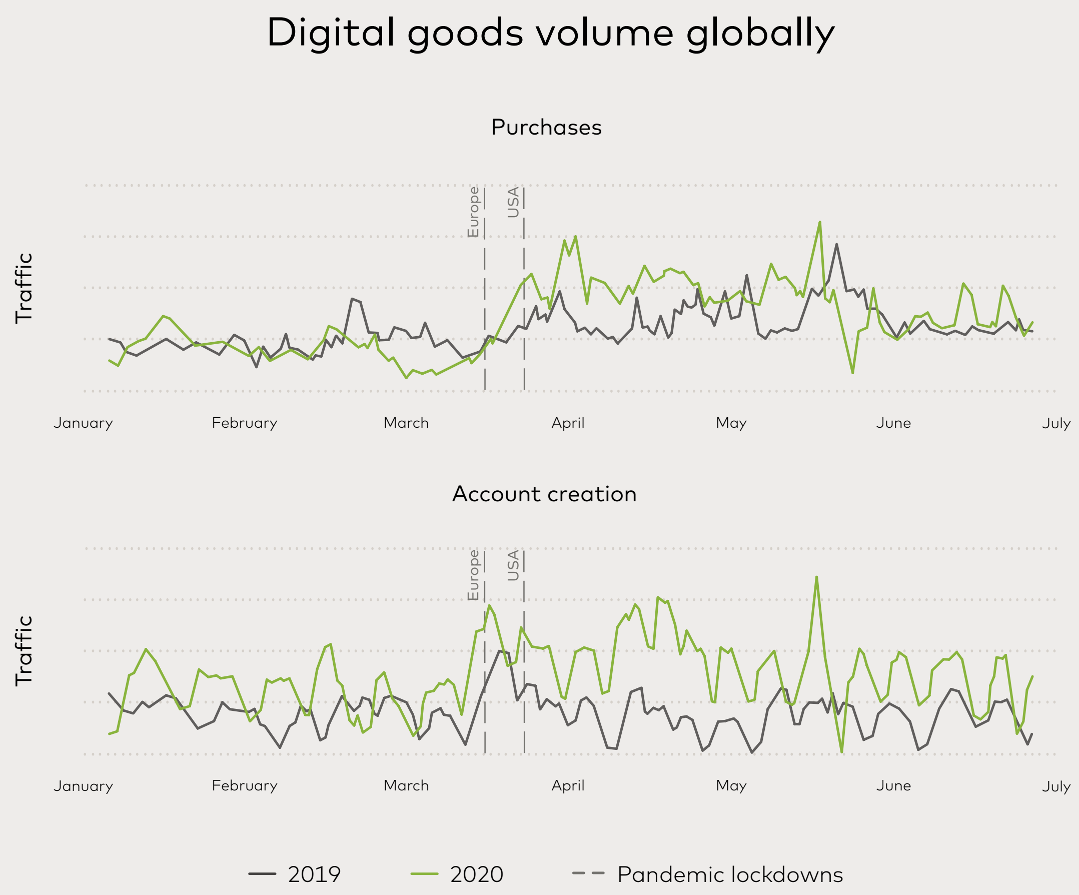


eCommerce traffic volume globally by placement, from January to July. Source: *NuData*

eCommerce and digital goods (cont.)

The account creation placement, where users create new accounts, had the sharpest year-over-year change. This growth was most likely due to new users moving to online services as physical stores closed and there was a need to open new accounts to access those services.

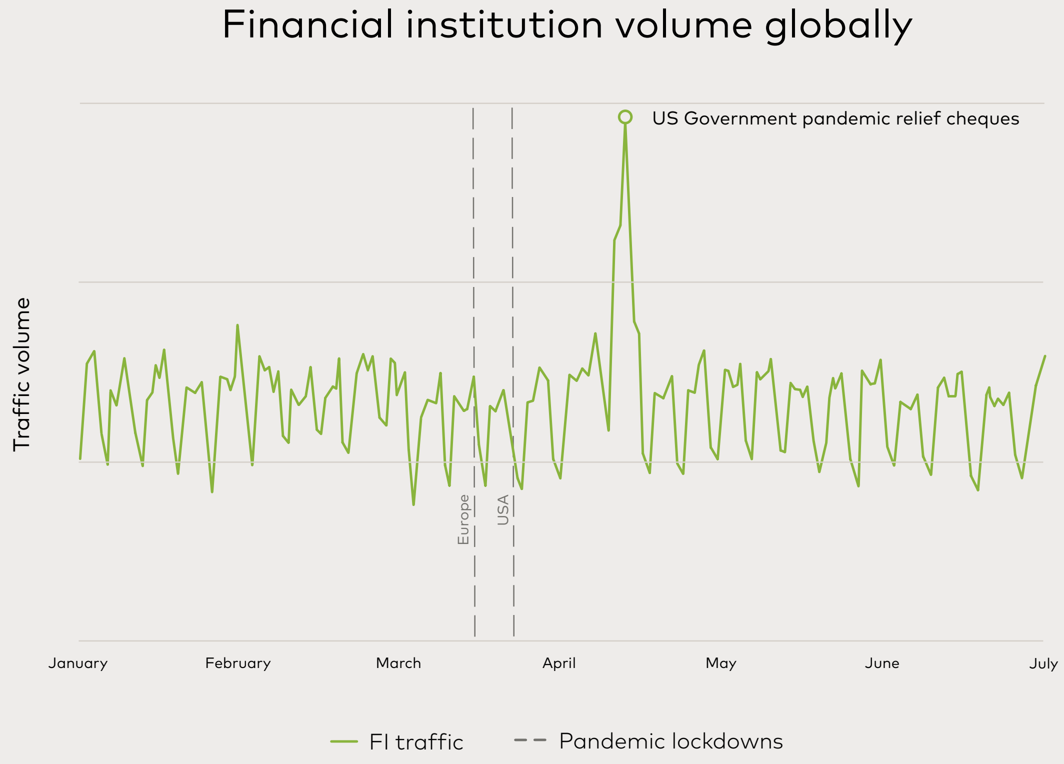
This increase in online demand is an opportunity for eCommerce and digital goods companies to invest and improve their security tools to enhance the user experience, helping users adapt to the online channel.



Digital goods traffic volume globally by placement, from January to July. Source: *NuData*

Financial institutions

Financial institution (FI) traffic remained stable. There was a clear spike in mid-April from customers accessing their bank accounts, partially influenced by the first round of U.S. economic stimulus checks, but otherwise, the volume from trusted users was steady throughout the first half of the year. However, high-risk traffic has remained unchanged during the pandemic, highly focused on targeting financial institutions with large-scale sophisticated attacks. This constant stream of attacks at institution's login placements underscores the need to protect every user endpoint continuously, regardless of the customer changes that may be happening in the online ecosystem.



Financial institution volume globally by placement, from January to July. Source: *NuData*

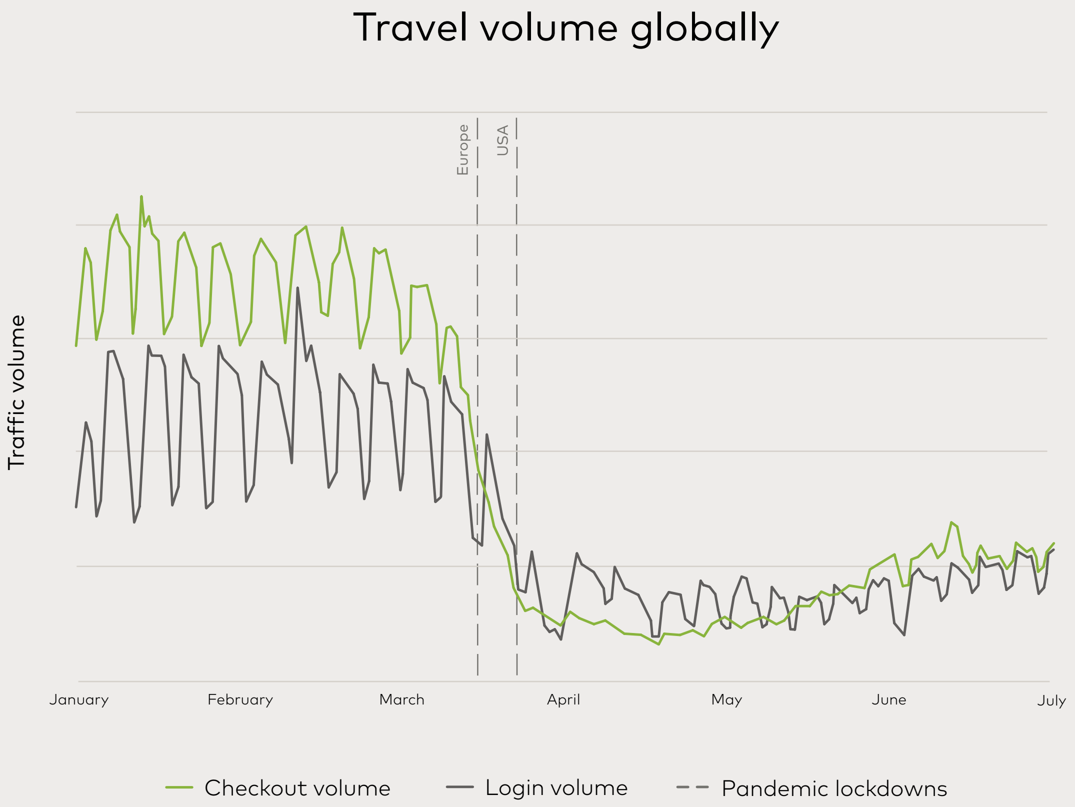
Travel

Travel industry traffic across all placements (interaction points such as account creation, login, and checkout) had a growing trajectory during January. However, it started to decrease in February, before coming to a halt in March. Mid-March showed a small uptick in traffic attributable to users logging in to cancel their bookings or change reservations.

Although this is one of the hardest-hit industries during the pandemic, its trusted traffic has started to regain momentum in May and June, increasing by 360% from its lowest point in April. This industry needs to keep the customer experience in mind as a priority to help its returning users.

360%

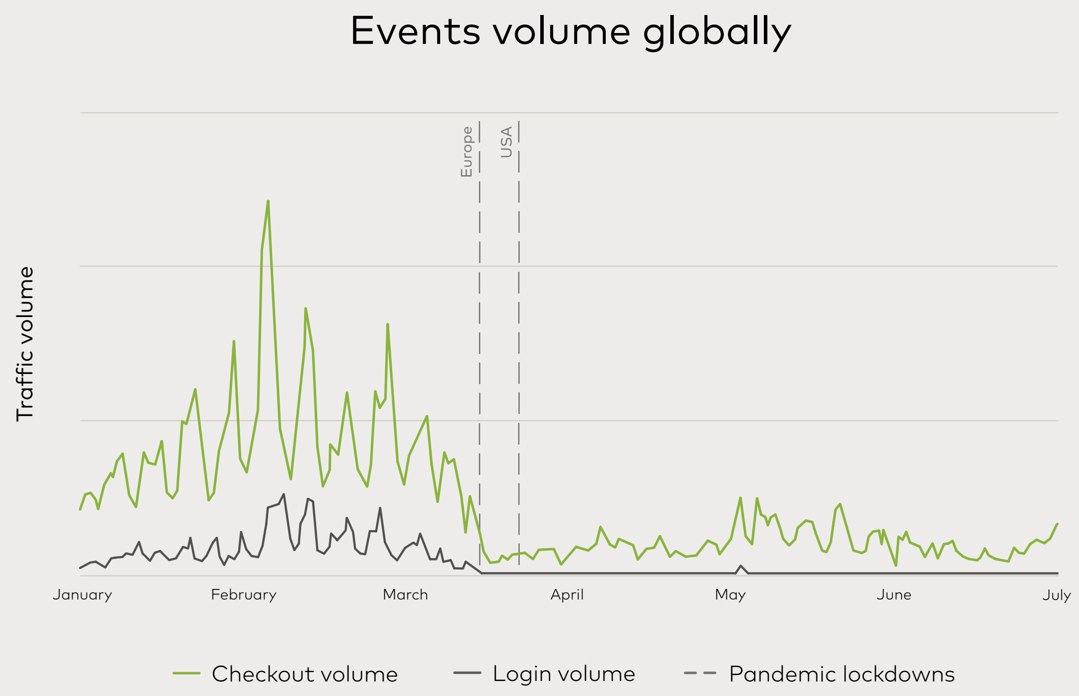
Traffic growth since lowest point in April



Travel volume globally by placement, from January to July. Source: *NuData*

Events

Events, such as concerts and sporting events, ground to a halt in March as social distancing became the norm. Unfortunately, this category continues to have little activity for the time being. However, fraudsters are still deploying attacks against companies with decreased traffic in the hopes that these companies have paused their security tools until their users start coming back. NuData is regularly finding mass-scale attacks that target industries with a drop in traffic, such as the travel and events sectors, as the user accounts in those companies still hold valuable information.



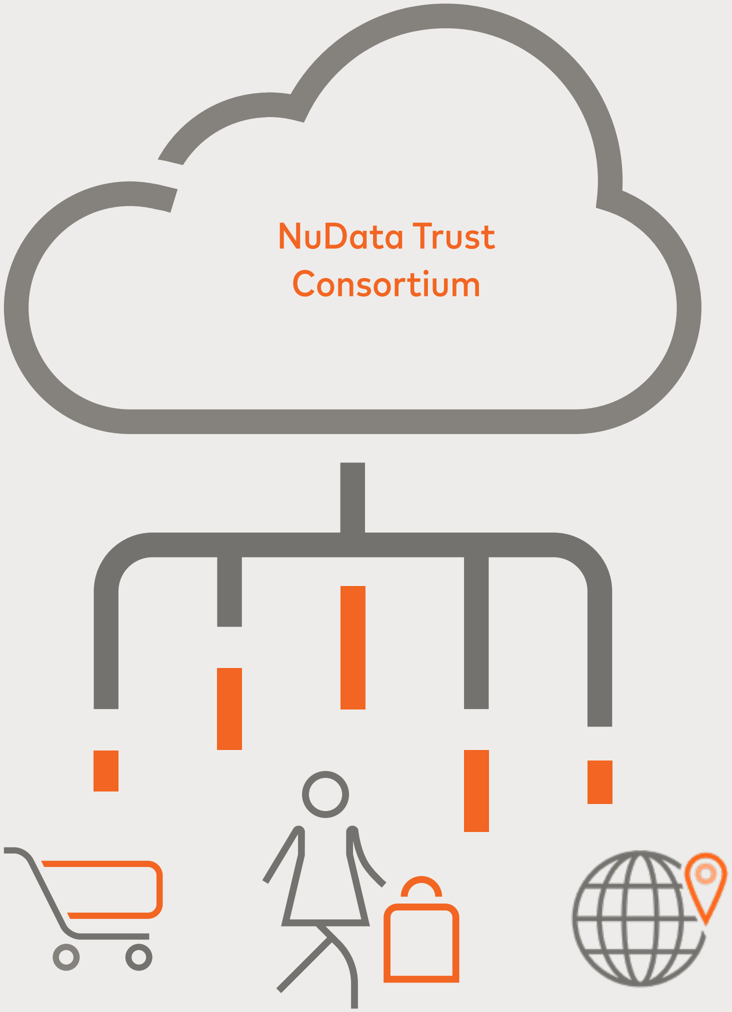
Source: NuData, 2020

Chargebacks during a pandemic

In situations of crisis, chargebacks tend to increase across eCommerce companies.

According to a recent report by Ethoca, a Mastercard company, and the Aite Group[1], the cost of chargebacks to U.S. issuers was already expected to grow from US$585 million in 2019, to more than US$690 million in 2020. However, this projection was made prior to the COVID-19 crisis that caused a surge in chargebacks and customer service disputes for certain industries.

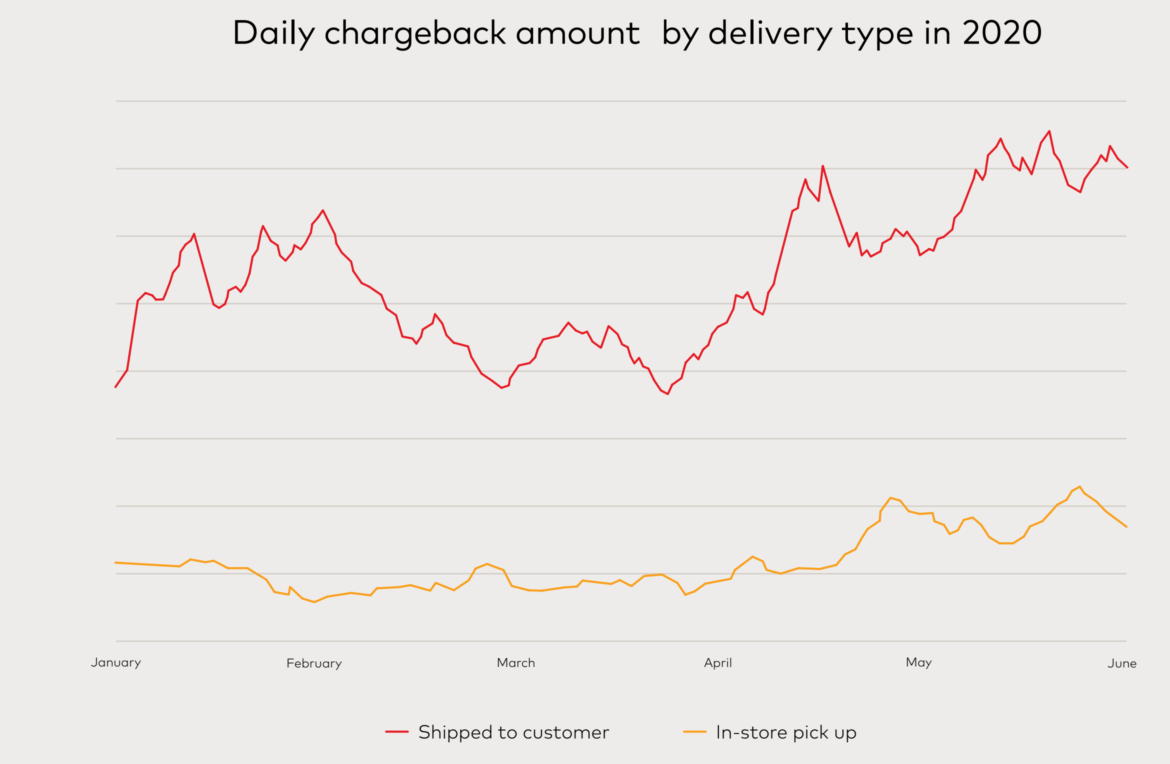
NuData analyzed eCommerce data from its Trust Consortium to explore the changes in chargebacks during the pandemic. The analysis takes us from January to the end of May of 2020, as chargebacks are reported an average of 30 days after a purchase is made.



[1] *Improving the dispute experience: Transparency is power.* An Aite Group research report sponsored by Ethoca, 2020.

To provide deeper analysis; chargebacks are divided by delivery type during 2020: purchases shipped to the customer address and purchases picked up at the store.

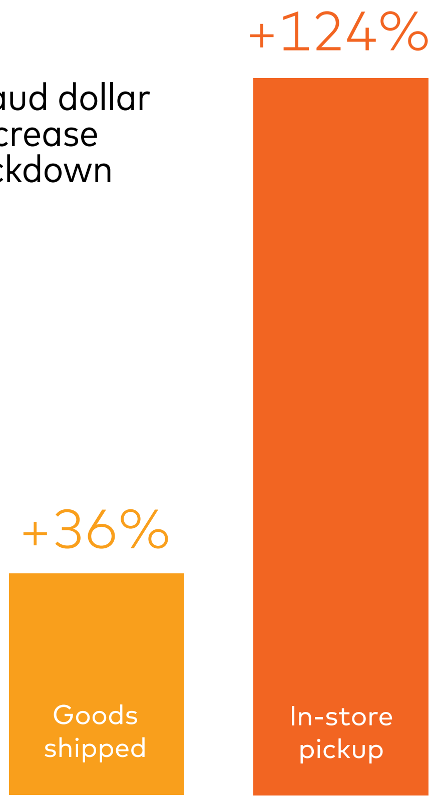
The chart shows peaks in chargebacks at the beginning of the year that correlates to holiday shopping and fraud. Then, the line for chargebacks from purchases shipped to customers trends down until March. In March, coinciding with the generalization of lockdowns, both types of chargebacks begin to trend up dramatically.



Volumes of chargeback requests from eCommerce purchases. Source: NuData, 2020

Although the volume of chargebacks from purchases shipped to customers remained the highest, chargebacks from goods picked up at stores grew the most – more than 100% growth in April. As chargebacks are requested after purchases are finalized, May results could still be higher than reported in this analysis.

Total fraud dollar value increase since lockdown



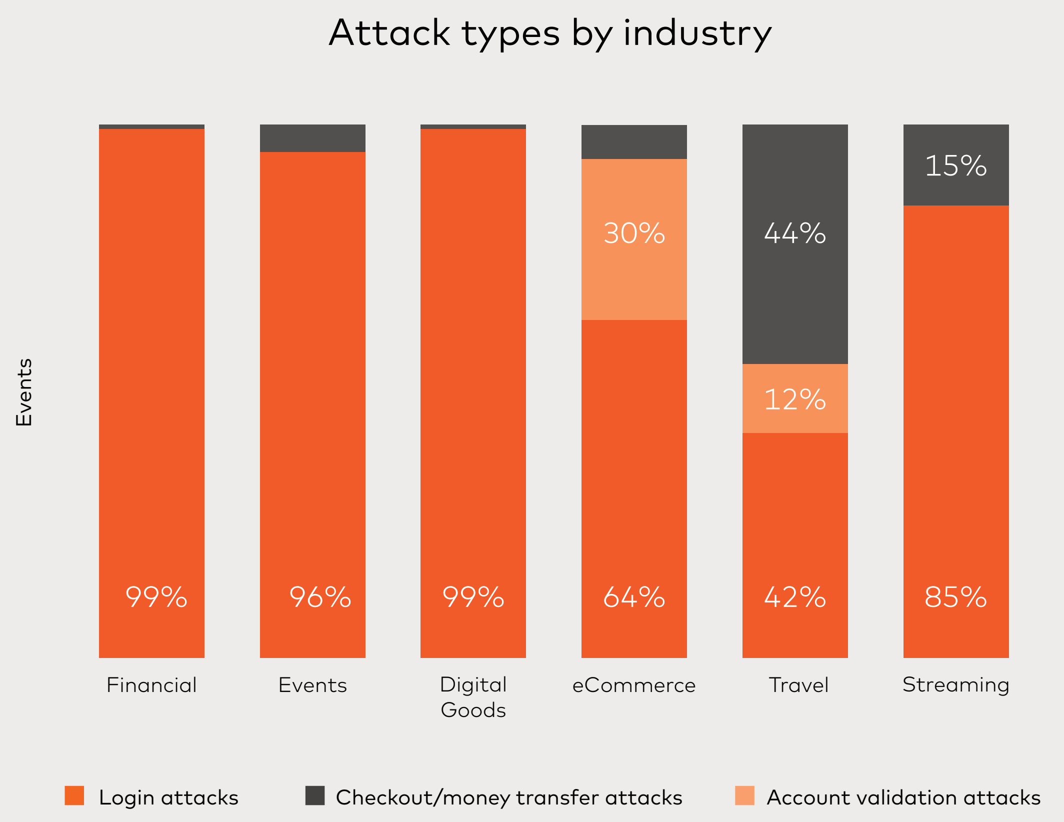
The total fraud dollar value pre and post-lockdowns (from January to March for pre-lockdowns and from April to May for post-lockdowns) increased by 36% for goods shipped to customers and 124% for in-store pickup.

Attack by customer placement

Looking at attack types by industry tells us what customer placements are at higher risk. Account takeover attacks (ATOs) at login make up most of the attack traffic.

This is unsurprising considering these attacks are deployed at a larger scale than others as login credentials are easier and cheaper to access than other types of user information.

Travel and eCommerce receive a wider variety of attacks, with travel showing an even distribution between attacks at login and checkout. During the lockdowns, these two industries exhibited the biggest fluctuation, with travel attacks at checkout climbing to 58% of total high-risk events in February and risky activity in eCommerce account validation pages (pages where customers can access information such as booking info, number of reward points, order status, or account profile) reaching 65% in March.



Source: NuData, 2020

Quality of stolen credentials by industry

Attacks at login use combinations of usernames and passwords, many of which are incorrect. Attackers deploy mass-scale attacks at login, such as credential stuffing, to test those credentials and determine which combinations open an account, known as hits.

When these attacks take place, NuData mitigates them with its behavioral technology before fraudsters know if their credentials work. NuData also evaluates the number of credentials that during an attack were correct and would have granted access to the account if otherwise not protected; this is called the success rate of an attack. This number gives an idea of the quality of the credentials bad actors have access to across industries. An example of bad data quality would be a username that doesn't exist on a platform or a password that doesn't work.

This summary shows the percentage of high-risk login attempts with correct credentials. Based on this summary, attacks targeting event or ticketing companies had the highest quality credentials at 4%, much higher than the cross-industry average success rate of 1.4%. This finding underscores the need for tools that can detect these account takeover attempts, as even a success rate above 1% can lead to thousands of compromised accounts from one single attack.

Rate of login attempts with correct credentials

Digital Goods	eCommerce	Financial Institutions	Travel	Ticketing/ Events
0.02%	1.18%	0.40%	1.37%	4.00%

1.4%

Cross-industry average success rate of high-risk login attempts with correct credentials

1%

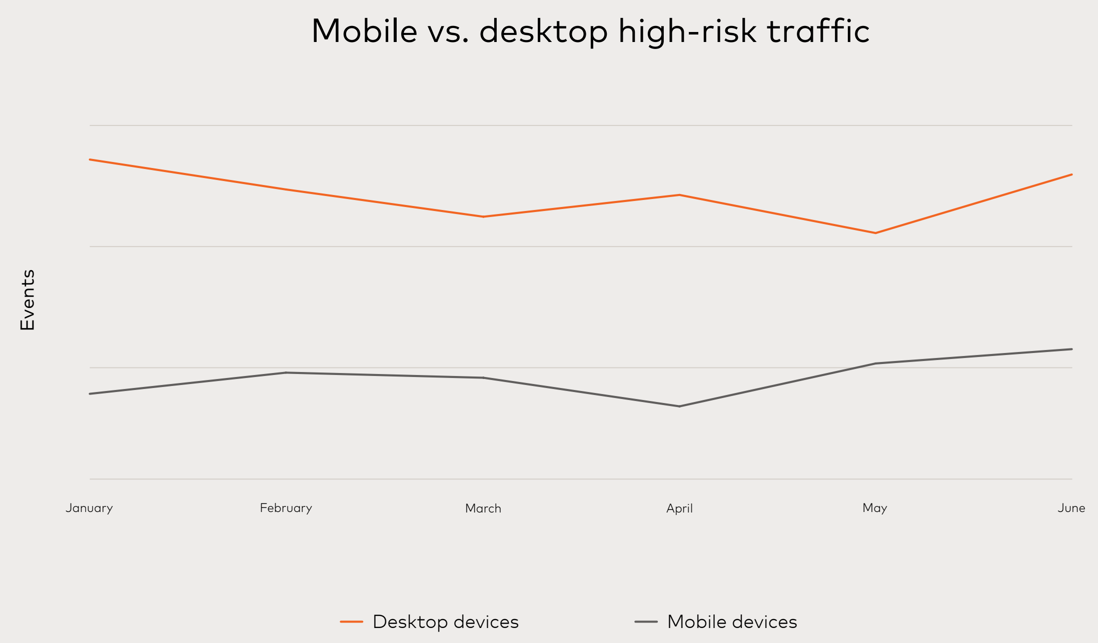
A success rate above 1% can lead to thousands of compromised accounts from one single attack

More attacks go mobile

While attacks on desktop continue at higher levels, attacks from mobile devices have been growing. This growth is reflected in the chart, indicating that high-risk mobile traffic grew by 55% in the first half of 2020.

55%

Growth of high-risk mobile traffic



Source: NuData, 2020

Conclusion: what the data tells us about 2020

1

Attackers have increased their use of sophisticated techniques to make their attacks count, especially when targeting financial institutions, but also across other industries. This is a natural evolution as bot-detection security tools have become better at blocking basic bot attacks. The inclusion of behavioral tools in the security strategy is helping companies detect fraud at every level, including human-looking attacks, and thwart these online threats.

2

With the world experiencing an unprecedented pandemic, commerce is increasingly moving online, and with it, bringing new users to the digital sphere. It's not surprising that many fraudsters responded accordingly. NuData found that although the volume of attacks at login remained stable, high-risk traffic at account-creation among some merchants increased in the first half of 2020 compared to 2019, primarily after lockdowns began. This growth is influenced by bad actors using new accounts to make fraudulent purchases or to buy sought-after and restricted goods at mass scale for later resale.

3

Looking at attacks by placement, most attacks across all industries happened at login with account takeover attacks (ATOs) the main threat. However, attacks in other industries such as travel were evenly distributed, with 44% of attacks happening at checkout and 30% of eCommerce attacks taking place at account validation pages (pages where customers can access information such as booking details, number of reward points, order status, or account profile). This variety of targeted placements highlights the need for companies to secure all the different user interaction points.

44%

Travel industry attacks are happening at checkout

High-risk traffic at account-creation among some merchants increased in the first half of 2020

30%

eCommerce attacks happening at look-up pages such as review points, purchase state, or card information

4

Analyzing individual attack vectors, we can find common patterns that can help prevent similar future attacks. Many of them use IP addresses or devices linked to past malicious behavior seen on the NuData Consortium. This underscores the value of machine learning and the Trust Consortium in recognizing previously-seen patterns in new attacks as well as recognizing risky parameters.

5

Once the lockdowns began in North America, the frequency of chargeback fraud in this region increased, more than doubling pre-COVID volumes (i.e., January to March). The dollar value of chargeback requests also increased considerably. These trends highlight the importance of tools that provide advanced notification of incoming fraud and customer disputes so that merchants can take action to resolve them before they become chargebacks.

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.

Account validation page: Any page within a platform where the user can look at their personal information and manage it, such as pages with reward points, payment methods, or an account profile.

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 characterize for 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.

Botnet: Internet-connected devices, each of which is running one or more bots to perform large-scales attacks.

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

eCommerce: Includes companies buying and selling goods or services online.

Events: 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).

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. They are highly organized and have significant resources at their disposal behavior and run scripts in the environment to simulate human interaction.

Spoofing: The act of disguising a communication from an unknown source as being from a known, trusted source. For example, the modification of a device's information such as operating system, browser, or version to appear as a different device.

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.

Travel: Includes companies with travel portals.

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

AWARDED

"Most Critical Solution in the Last 30 Years"

of cybersecurity by SC Magazine

+650B

behavioral events monitored in 2019

+100M

accounts protected monthly

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 analyzing over 650 billion behavioral events only in 2019, 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.

NuData Security
mastercard