Fraud.net

The New Normal for Cybercrime

Fraud in the COVID Era

Table of Contents

Introduction: How Rapid Digitization in the COVID Era Created a Cyber Crime Gold Rush

In fragile times, fraud flourishes. Therefore, it’s no wonder the COVID-19 pandemic created an ideal environment for global fraudsters.

62%

Global growth in ransomware between 2019-2020

46%

Growth in Digital Transaction Fraud between 2019-2020

Whether it’s phishing attacks and ransomware or stealing credit and debit card info, the Dark Web has never been so “bright.” As MonsterCloud’s CEO Zohar Pinhasi chillingly put it, criminals during COVID just “stepped into a gold mine.”

COVID-19 not only destabilized world economies, it drove everyone online. People that couldn’t or wouldn’t adapt to digitization have been left in the dust. While these new technologies offer customers and businesses many advantages, they also increase the risk of cybercrime. The rapid adoption of digitization coupled with economic and health fears has created the perfect opportunity for online opportunists. Now more than ever, corporations and individuals need robust fraud resilience to combat increasingly complex threats.

The Scale of the Problem

4,000

Cyberattacks per day in 2020

400%

increase since 2019

300%

increase in people paying ransomware since 2019

$675 million

US losses to COVID-related fraud attacks in 2020

Just How Much Has Fraud Grown Since COVID-19?

The statistics don't lie: COVID has directly affected global fraud activity. Indeed, according to TransUnion's 2021 Global Consumer Pulse Study, digital transaction fraud rose 46% between 2019 - 2020 and 2020 - 2021. Researchers also found that reported digital scams related to COVID-19 have increased from 29% in 2020 to 36% in 2021.

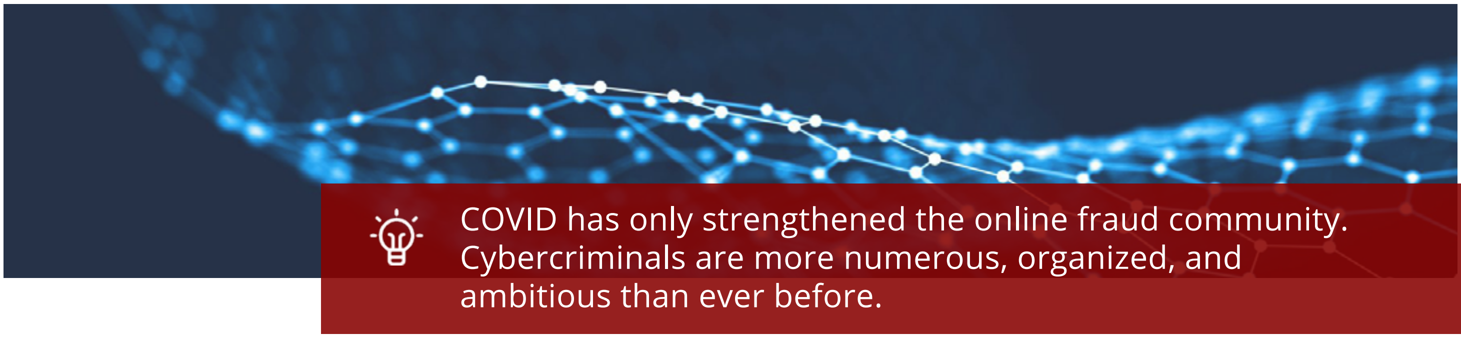
In the United States, the FBI claims it had to respond to 4,000 cyberattack claims per day in 2020. For context, that's up roughly 400% from 2019's average.

Another startling report from the Institute for Security and Technology found that the number of people who paid for ransomware rose 300% between 2019 and 2020. Additionally, the 2021 SonicWall Cyber Threat Report found that ransomware attacks have gone up 62% worldwide between 2019 - 2020, and in the US alone, this percentage jumped over 150% .

Many ransomware experts believe these high-priced attacks are inspiring countless copycat cybercriminals. In the chaotic atmosphere of the COVID pandemic, fraudsters have upped their game, and they aren't afraid to target governments, hospitals, or major supply chains. Plus, as people face financial hardship due to COVID, it's more likely they will turn to cybercriminal activities to support themselves.

As Fraud.net noted in a recent report, collaboration on the Dark Web is a significant factor driving the increase in COVID fraud. Cybercrime-as-a-Service is a growing industry, and it's increasingly difficult to detect. Many fraudsters know how to use privacy technologies like VPNs to obscure their activities.

There have never been so many people online at the same time, including on sites with illicit activity. In fact, the firm Sixgill found Dark Web visitors shot up 44% in the early days of COVID-19 lockdowns. While the study highlights that most of the criminal activity was related to only about 20% of Dark Web posters, it shows there are plenty of opportunists interested in fraud related activity.

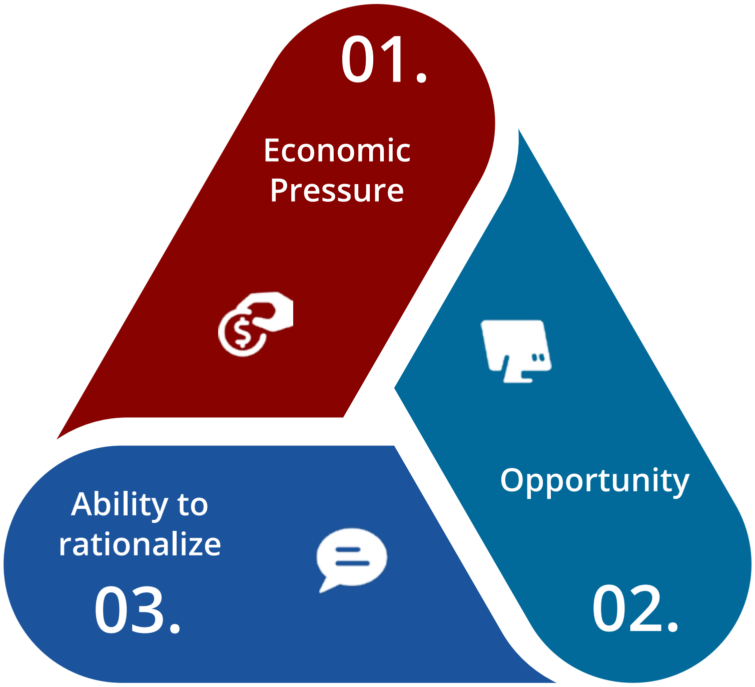


COVID has only strengthened the online fraud community. Cybercriminals are more numerous, organized, and ambitious than ever before.

Why Has Fraud Grown So Much During COVID-19?

Whenever there's an economic downturn, there's typically an uptick in fraud. Info from the Association of Certified Fraud Examiners (ACFE) shows that 80% of anti-fraud businesses saw more fraudulent activity during tough economic times. Understandably, in desperate scenarios, more people could be tempted into criminal activities.

The ACFE also reminds companies that the "Fraud Triangle" can explain why people resort to fraud. According to this model, entities are more likely to engage in fraud if they feel pressured, see an opportunity, and can rationalize their actions. All three of these conditions certainly ring true for many people in the COVID era, considering that Pew Research found that 25% of adults in the USA say at least one person in their home got laid off due to COVID-19.



The Fraud Triangle

While these explanations are helpful, we must remember the COVID-19 pandemic is so much more than an economic issue. First and foremost, COVID is a health emergency. Given the increased concern surrounding health issues, fraudsters could more easily scare people with sophisticated phishing attacks. Indeed, the Federal Trade Commission estimates Americans lost about $675 million in COVID-related fraud attacks in 2020, falling victim to these scams. Sadly, many of the most lucrative phishing attempts targeted the elderly.

Another ripple effect of COVID that worked in fraudsters' favor was the transition to a digital economy. COVID forced everyone to move to a more virtual presence, which means more data than ever before is up for grabs. Companies with inadequate digital fraud protection saw major losses and data breaches as a result. For instance, UNCTAD recently found that eCommerce

> “
> Friendly fraud increased by 43% over the last few years.

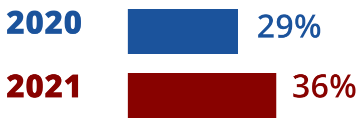
has increased to 17% of the global retail market from 14% in 2019. Consequently, friendly fraud increased by 43% over the last few years, and analysts don't expect this trend to slow anytime soon. Not only are more people interacting with eCommerce platforms; many employees nowadays are working from home. When people work from home, they don't enjoy the same protections of an integrated office, such as secure siloed work computers or protected networks; yet another reason for the uptick in COVID fraud.

Lastly, another contributing factor to the rise in COVID fraud could be the lack of proper funding. Countless businesses have had to cut corners to survive during COVID, and usually that means reduced spending on cybersecurity. However, offices need to ramp up their spending during challenging times to deal with increasingly complicated threats. A “lowered shield” simply makes it easier for criminals to get in.

What Are The Top COVID Scams?

So, what are the major crimes during the pandemic? Unsurprisingly, digital fraud is regarded as the highest concern by security experts. Anti-fraud experts in a 2020 ACFE survey reported that cybercrime was the top threat in the COVID era. Other issues respondents had concerns about included payment fraud, bribery, and embezzlement.

COVID related scams rose in 2021



Two attacks stood out: **phishing** and **ransomware**. According to Microsoft, about 20,000-30,000 themed phishing attacks related to COVID were reported every day in the USA during 2020. As for ransomware, companies reported that attacks have grown by at least 800% during COVID-19.

Additionally, an illuminating survey from card issuer Marqueta revealed 52% of customers in the UK and USA had to deal with credit card fraud in 2021. The company also noticed a 20% rise in stolen debit card info between 2020 and 2021.

However, the most glaring year-on-year increase was related to criminals who stole personal data to create false online accounts. The number of people who reported this issue increased by over 120% from 2020 to 2021.

What Long-Term Impacts Could We Expect From COVID Fraud?

At least 16% of the US workforce, or nearly one in five workers, could remain at home for years after COVID-19 passes.

Digital fraud will likely become an ever-present threat in the “new economy,’ considering the Deloitte survey that found over 60% of independent directors claim fraud will increase at least two years down the line.

Despite the world’s slow re-opening to in-person activities, the trend towards digitization probably won’t wane in the post-pandemic era. Recent data from Visa found that consumers’ preferred payment methods are changing: Almost 50% of customers claim they will only visit stores if they have contactless payment options such as buy online, pick up in store (BOPIS). Even more shocking, about 78% of respondents said they had already changed their payment methods to digital options to better align with personal safety from COVID.

Another issue workers face in the post-COVID world is the new stay-at-home workforce structure. In 2020, the Harvard Business School said the work-from-home world isn’t going anywhere anytime soon, as more people prefer this model versus traditional office settings.

In fact, according to Harvard’s analysis, at least 16% of the US workforce could remain at home for years after COVID-19 passes. Unfortunately, the lack of safety infrastructure in at-home offices and the rise in eCommerce means everyone is at greater risk for fraud during and post-COVID. Also, invoice fraud will become increasingly difficult to detect when employers have to pay their employees remotely.

How Could Companies Prevent Pandemic Fraud?

It's clear that companies need to be proactive about countering COVID fraud. However, that doesn't mean simply hiring a few extra staff members onto your fraud detection team will help. Many of today's cybercriminals are using sophisticated technology to manage their criminal enterprises, and mere manual labor isn't enough to track these types of fraud attacks.

The best way to stay on top of these novel threats is to enhance your team's technical capabilities, such as investing in Machine Learning and AI. Supervised and unsupervised Machine Learning infrastructure helps spot anomalies in your reporting that human eyes would likely miss.

One of the keys to this system's success is its large pool of data. AI and Machine Learning programs can hold immense amounts of info as they cross-reference all of your financial transactions. Also, these systems "learn" from their past analyses and auto-adjust, so fraud teams don't have to constantly update their systems manually as new threats arise.

FRAUD.NET PROVIDES MORE EYES FOR YOUR FRAUD DETECTION TEAM

Fraud.net wants to keep you free from online fraud. To meet the immense challenges posed by post-pandemic fraudsters, Fraud.net has developed one of the most robust AI-based anti-fraud platforms. Our products and AI services provide fraud resilience at all the most vulnerable points, such as login, emails, transactions, and applications.

Customers can choose what tools work best for their business needs. These Machine Learning systems include Linked Entity Analysis, which was designed to tackle the increasingly collaborative nature of cybercrime.

With more data in your fraud detection pool, you'll have a better chance of ensuring a safe digital experience for your enterprise.

Manage COVID Fraud with the AppStore

The best approach to combating online fraud is a comprehensive one - cybercrime comes in a variety of forms, so you must leverage a variety of APIs to combat them. Fortunately, Fraud.net's AppStore offers you access to third party integrations, where you could merge your data with our extensive API library. With more data in your fraud detection pool, you'll have a better chance of ensuring a safe digital experience for your enterprise.

With one seamless connection, our AppStore allows you to leverage 25+ data partners and billions of insights for comprehensive risk management.

On a single unified platform, screen identities, Tax Identification Numbers, account information, and more against our Collective Intelligence Network with our AppStore partners, such as Jumio, TINCheck, and DIRO. Additionally, avoid vendor fraud by screening new third-party vendors and testing them in a fraud prevention sandbox before onboarding them.

No longer do you need to contend with siloed platforms or data - view all of your fraud prevention data within one single unified platform.

One Seamless Connection

25+ Data Partners

Billions of Insights

Fight Phishing and Ransomware with Email AI

To combat these prominent fraud schemes of the pandemic, an inbox monitoring service is key for flagging potential phishing, invoice fraud, or ransomware emails.

Fraud.net's Email AI easily integrates with Outlook to screen incoming emails and verify email addresses, geolocation of the sender, and frequency to ensure that you only open legitimate, safe emails. With state-of-the-art accurate risk scoring, you can navigate your inbox with peace of mind, and with every approval or denial, the AI-powered tool learns and adapts to your needs.

Gain control of your emails and avoid costly phishing, ransomware, and business email compromise scams with our AI and machine learning based products.

PUT FRAUD.NET'S ADVANCED AI ON YOUR SIDE

There's no way to avoid digitization, which also means businesses can't avoid dealing with online fraud. The only way to combat the increasingly sophisticated world of fraudsters is to put the latest anti-fraud technology on your side. Fraud.net allows you to take advantage of the latest innovations in AI fraud detection for a seamless and successful anti-fraud program.

No matter what industry you're involved in, there's a good chance Fraud.net has experience in your field. Our team has integrated AI fraud detection into fintech, government, e-commerce, and gaming companies, to name a few. Plus, in 2021, Gartner acknowledged Fraud.net as a leader in Online Fraud Detection. Clients can rest assured Fraud.net will work tirelessly to combat the immense challenges posed by COVID fraud.

If you're hesitant about upgrading to AI fraud detection, please give Fraud.net a call for a demo. Our team would be happy to share our products and expertise with your business.

REQUEST DEMO