



**Q1 2021 TRUST & SAFETY INDEX**

# Exposing the Multi-billion Dollar Fraud Economy



# Contents

3

Confronting the Impact of a Booming Fraud Economy

4

The State of Payment Fraud: Vertical trends and insights

7

Old Tricks, New Schemes: Automated attacks and counterfeit accounts

11

Scaling Fraud Operations with Digital Trust & Safety

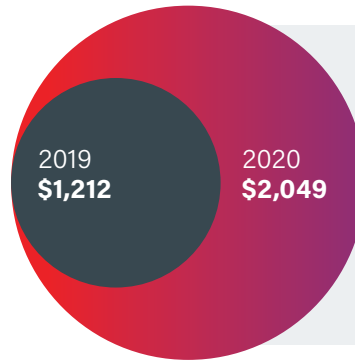


STATE OF PAYMENT FRAUD

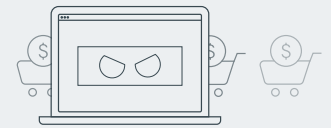
# Vertical trends and insights

The pandemic played an influential role in how payment fraud changed and scaled in 2020. Incidentally, the relentless disruption felt across e-commerce also exposed the depth of the Fraud Economy, and the danger it poses for businesses. It's more than a blanket term for online crime; it's a sophisticated network of active cybercriminals with access to everything they need to exploit online businesses—and it operates on the same basic principles as the industries it impacts.

As a result, fraudsters are as knowledgeable about the mechanics of digital commerce as the legitimate merchants they target. They can accurately identify security vulnerabilities, and know how to use a merchant's success against them. As internet traffic surged last year by between **50%-70%**, the amount of money spent by online shoppers **nearly doubled**. Fraudsters seized on climbing transaction volumes and unanticipated consumer behaviors like stockpiling, driving the average value of attempted fraudulent purchases up by **69% year-over-year**.



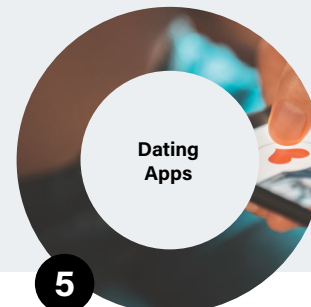
**Average Fraudulent Order Value increased 69%**



Fraudsters' growing willingness to work together also contributes to the Fraud Economy's steadily-growing reach and complexity. In 2020, every market experienced some level of uncertainty or unexpected shifts in demand, and fraudsters were quick to exploit those changes: when traffic tanked in transportation, cybercriminals attacked dormant accounts for rewards points and payment data. Conversely, when volumes swelled in gaming and crypto, fraud rates *still* rose—the byproduct of fraudsters banking on risk teams being too overwhelmed by surging traffic to catch them all.

## 2020 Top Targets: 5 highest fraud rates by vertical

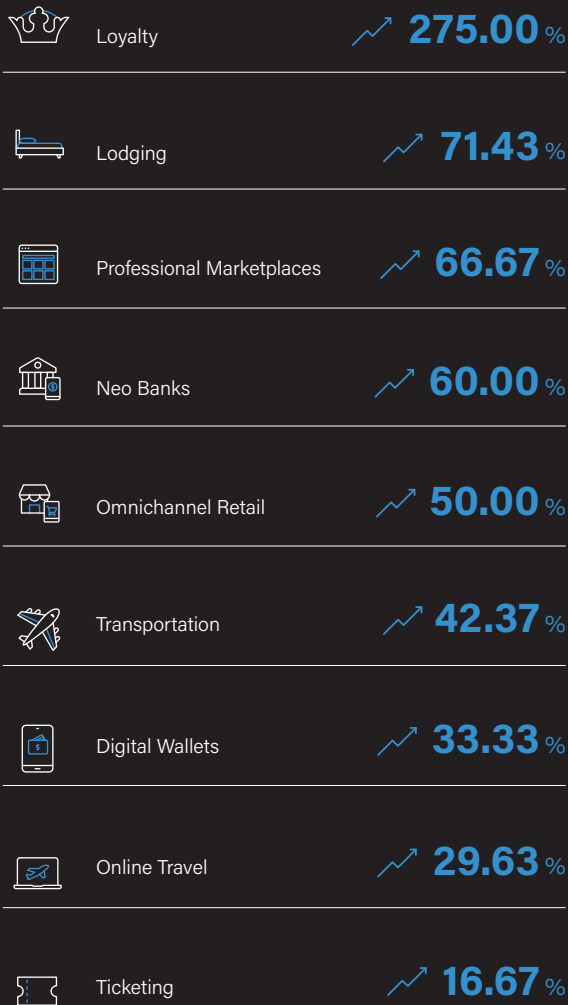
In 2020, transportation reached an **8.4% overall attempted fraud rate**, while crypto exchanges and gaming/gambling followed with fraud rates at **4.6%** and **3.7%** respectively.



Attempted fraud ballooned across Sift's data network, driving year-over-year fraud rates wildly high in some industries. Loyalty merchants, which help businesses engage their customers, saw fraud rates jump by **275%** as compared to 2019.

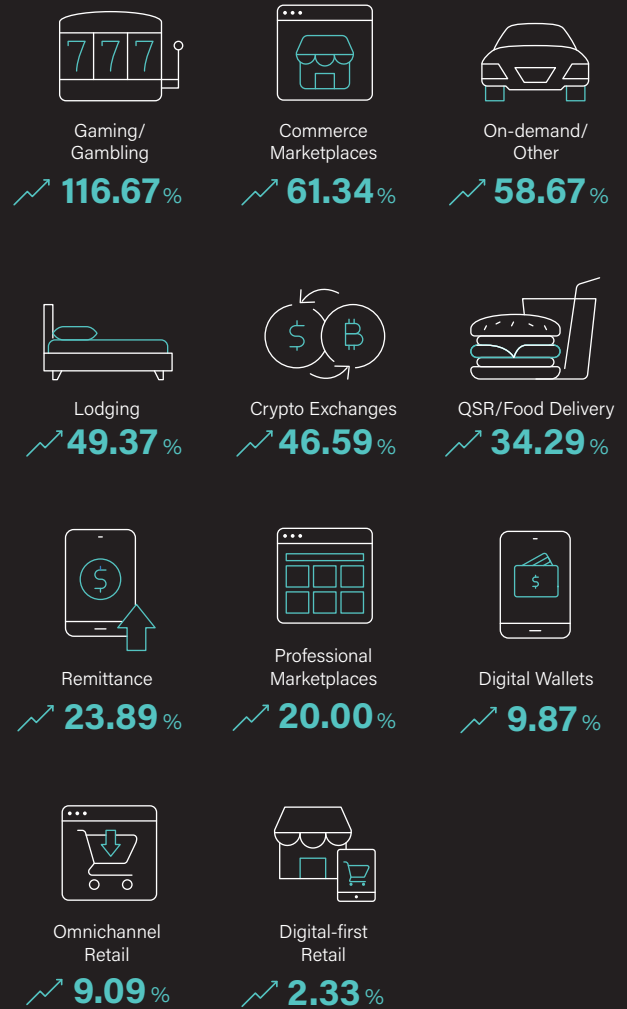
## Rising Fraud Rates: Top industries impacted in 2020

2019-2020 fraud rate increase



## YoY Rising Average Fraudulent Order Values

2019-2020 avg. fraudulent order amount increase



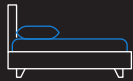
Fraudulent order values generally rose in tandem with expanding traffic. Gaming/gambling merchants were hit with illicit orders that doubled in value from 2019, followed by commerce marketplaces (similar to Etsy), on-demand services, lodging, and crypto exchanges, which saw illegitimate transactions grow by nearly half or more.

Four types of businesses were hit particularly hard by the burgeoning Fraud Economy: lodging merchants, omnichannel retailers, digital wallets, and professional marketplace companies each saw fraud rates *and* fraudulent order values rise considerably between 2019 and 2020—a problem compounded by pandemic-era market fluctuations.

Sift's Trust and Safety Architects credit these higher-value attacks and ballooning fraud rates to the challenges e-commerce businesses faced under coronavirus restrictions: too many people cooped up at home, misinformation causing changes in consumer behavior, dormant user accounts, and fraudsters watching from the wings, ready to take advantage.

## Hardest-Hit Industries: Where fraud rates and illicit order values are rising

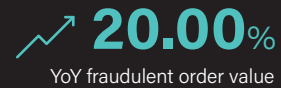
- 2019–2020 fraud rate percent increase
- 2019–2020 avg. fraudulent order value percent increase



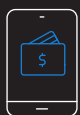
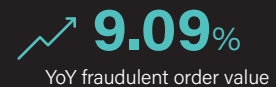
Lodging



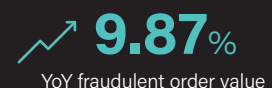
Professional Marketplaces



Omnichannel Retail



Digital Wallets



# Old Tricks, New Schemes: Automated attacks and counterfeit accounts

Bigger, faster, and more valuable online fraud attacks, happening across multiple verticals, are a clear sign of automation at work. Bots, scripts, and malicious software make the grunt tasks of cybercrime simple, and allow fraudsters to do more damage in less time. It's specifically useful for accelerating card testing and credential stuffing—an easy route to pilfered profits, given that **65%** of consumers repurpose usernames and passwords across multiple sites and services.

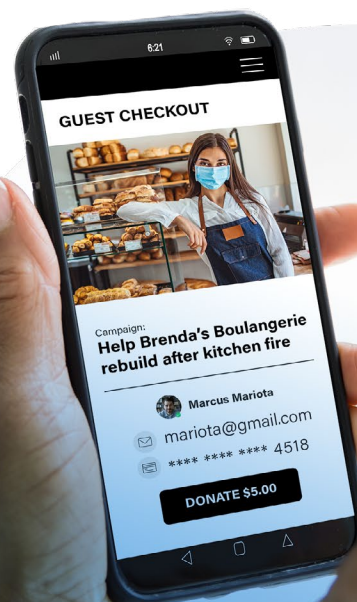
But the combination of tech and new tactics is causing the most concern among industry experts—fraudsters are weaving them together to supercharge new, sophisticated patterns of attack. Recently, Sift's Data Science team identified a prime example of the Fraud Economy in action: a money-laundering fraud ring, dubbed Cart Crasher by Sift, targeting donation sites during a time of global turmoil and need—and subsequently, rising traffic worldwide.

In 2020, the pandemic drove online giving up by **20.7%**, providing cover to fraudsters who “hide” behind traffic and

transaction surges, knowing that many merchants won't be equipped to handle scaling demand *and* rising fraud simultaneously.

Using stolen credit cards, fake accounts, and automated scripts to do the dirty work, this fraud ring repeatedly funneled small amounts of money to themselves by setting up fake causes on various giving sites in order to request donations. After creating a separate recipient account to link to those funds, the fraudsters involved would use guest checkout—entering fabricated emails or usernames as verification—and stolen payment information to “donate” small increments of money to their own fake causes (typically around \$5 USD).

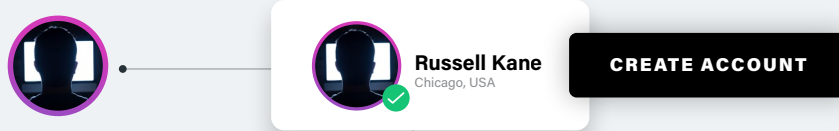
With automation to execute these illicit transactions at inhuman speed, it's a scheme with the potential to cheat merchants and consumers out of thousands of dollars—and allow fraudsters to use those ill-gotten gains to buy more stolen data on the dark web.



# Unwelcome Guests: Fraud ring launders dirty donations

Global fraud ring exploits pandemic struggles

Sift's Data Science team identified a money-laundering fraud ring targeting donation sites. Using stolen credit cards, fabricated accounts, and automated scripts, they repeatedly funneled small amounts of money using guest checkout, "donating" money to their own fake causes.

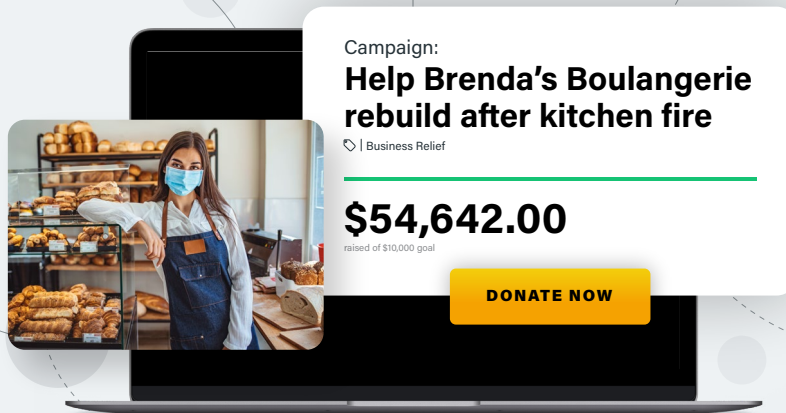


**Russell Kane**  
Chicago, USA

**CREATE ACCOUNT**

1 Fraudster creates recipient account

2 Fraudster publishes fake fundraising cause



Campaign:  
**Help Brenda's Boulangerie rebuild after kitchen fire**  
Business Relief

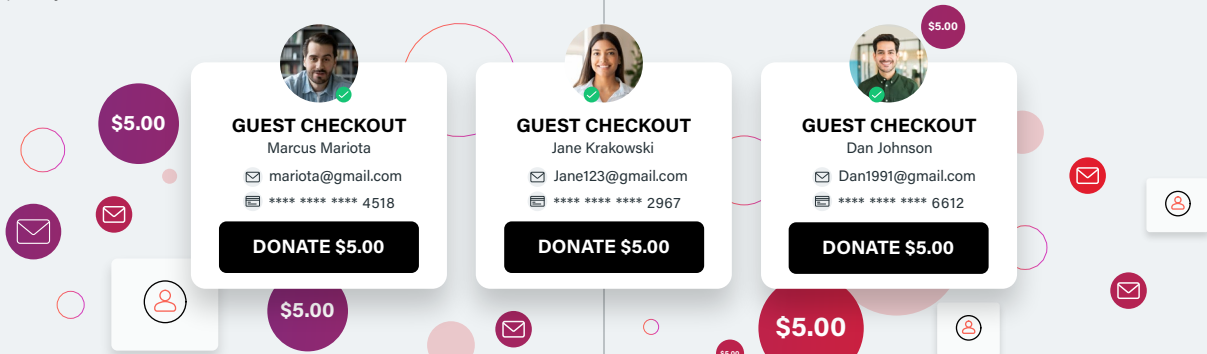
**\$54,642.00**  
raised of \$10,000 goal

**DONATE NOW**

Cybercriminals test the viability of stolen credit cards using low-value transactions, typically ~\$5 USD.

3

Using stolen payment details, fraudsters "donate" money via guest checkout to their own fake causes.



**\$5.00**

**GUEST CHECKOUT**  
Marcus Mariota  
mariota@gmail.com  
\*\*\*\* \* 4518

**DONATE \$5.00**

**\$5.00**

**GUEST CHECKOUT**  
Jane Krakowski  
Jane123@gmail.com  
\*\*\*\* \* 2967

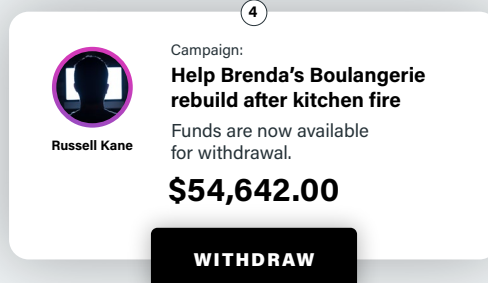
**DONATE \$5.00**

**\$5.00**

**GUEST CHECKOUT**  
Dan Johnson  
Dan1991@gmail.com  
\*\*\*\* \* 6612

**DONATE \$5.00**

4



**Russell Kane**

Campaign:  
**Help Brenda's Boulangerie rebuild after kitchen fire**  
Funds are now available for withdrawal.

**\$54,642.00**

**WITHDRAW**



## Summer Schemes and In-app Abuse

Payment fraud always arrives in spikes and valleys across e-commerce, and evidence suggests that fraudsters execute their most damaging, expensive attacks under the umbrella of increasing traffic and transactions; it would follow that the holiday season would be prime time for fraud. But last year's fraudiest day happened on **June 26th**—about 6 weeks earlier than 2019's fraudiest day of August 11th—suggesting that cybercriminals are prepared to exploit predictable changes in order volumes and values that take place year round.

**Day with highest attempted fraud rate**



Fraudsters follow the money and the market. Mobile shopping was set to hit over **\$284 billion** (45% of the total U.S. e-commerce market) last year, and well over half of payment fraud in 2020 was attempted via mobile device, increasing by **11% YoY**. Conversely, desktop devices were only utilized in about one-third of payment abuse incidents—a **10% drop** from 2019.

### Fraud On-the-Go

Device types that fraud occurs from

- Mobile **62%**  
*(iOS + Android)*
- Desktop **36%**  
*(Mac OS, Windows, Linux, etc.)*
- Other **2%**  
*(Consoles/other platforms)*

Fraudsters are drawn to the convenience offered by mobile devices and apps, emboldened to shoot for more valuable targets far more frequently. But that's not the only thing indicating that cybercriminals are focusing less on careful, covert crimes and more on getting what they want however they can. Sift's Trust and Safety Architects recently uncovered an **emerging fraud scheme** taking place on the instant messaging app Telegram, where professional fraudsters are teaming up with opportunistic online criminals via chat forums, in order to defraud delivery apps—in full view of the public.

And while food and alcohol are only fourth on the list of fraudsters' favorite items to buy with stolen funds, the velocity and volume with which grocery, delivery, and fast food orders occur (especially during the pandemic) makes it an extremely lucrative industry to attack. Topping that same list for different reasons are video game virtual currency, cryptocurrency, and site credits—digital payment types that only function in specific online environments, but that hold tangible cash and resale value.

### Fraudster Favorites: Top items purchased with stolen info



**01** Video Game Currency



**02** Cryptocurrency



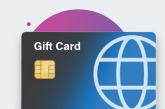
**03** Site Credits



**04** Food + Alcohol



**05** Event/Tour Tickets



**06** Gift Cards

## Category Hits: Highest-value attempted fraudulent purchases



Watches  
**\$5,000,000**



Cryptocurrency  
**\$484,000**



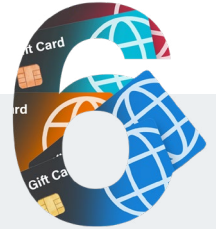
Event Tickets  
**\$53,264**



Political Donations  
**\$50,000**



Flights & Hotels  
**\$27,000**



Gift Cards  
**\$5,000**

The goods fraudsters go after with the money they steal aren't especially unusual, but the *amount* they're attempting to spend on them is striking. And, while these items don't appear to have much in common, they all share something critical to fraudsters on the hunt: they're tough to trace, hard to return, and worth more than their monetary retail value alone. Each of these goods can either be digitally laundered or physically resold for an even greater profit—including the top-targeted Patek Philippe luxury watches.

Collectively, 2020 Sift network data illustrates a thriving Fraud Economy that grows more sophisticated, efficient, intricate, and costly by the hour. As e-commerce matures globally and businesses individually scale, they'll naturally attract more customers—customers complete with credentials, credit cards, and user-generated content that fraudsters see as untapped opportunities for financial gain.

Payment abuse may be a core component of most cyberattacks, but to effectively prevent it, fraud teams need a broader understanding of vectors beyond stolen credit cards and cash. Spam, scams, fake content, account takeover, promo abuse—and more recently, fraudsters using these vectors concurrently—all act as gateways for fraudsters to undermine online security measures and hijack data. Without

an advanced, end-to-end solution that successfully identifies and stops all types of abuse, trust and safety analysts will forever be left to face an enemy they don't fully understand or know how to fight.

### Fraidiest Payment Types in 2020



**01**  
Gift Cards



**02**  
Store Credit



**03**  
Cryptocurrencies



**04**  
In-App Purchases



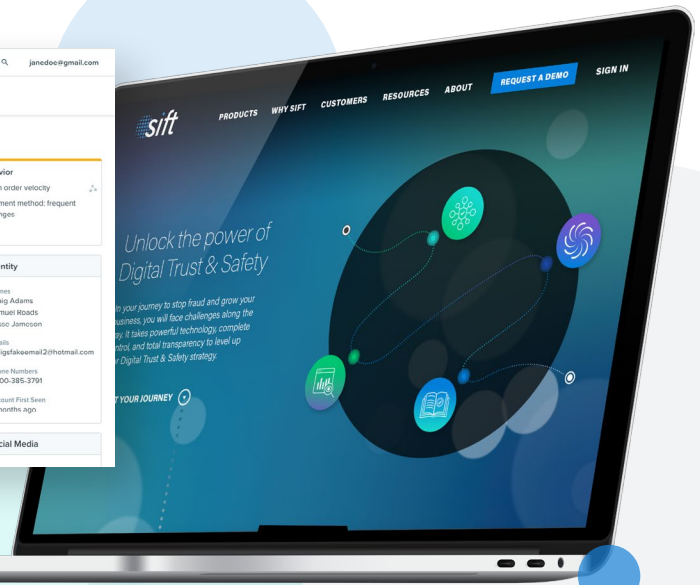
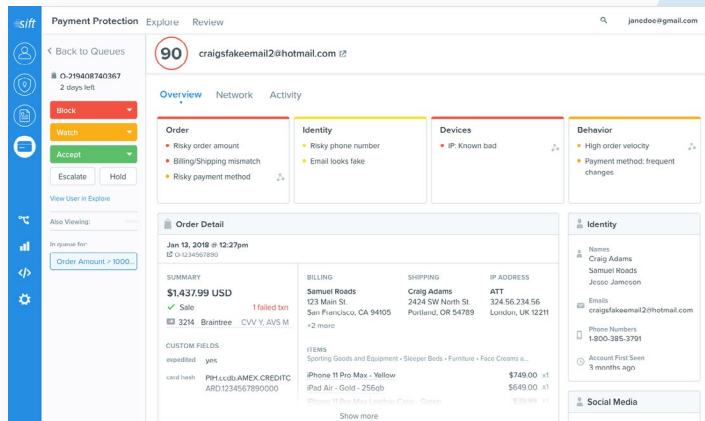
**05**  
Credit Cards

# Scaling Fraud Operations with Digital Trust & Safety

Cybercriminals have demonstrated that they can, and will, apply sophisticated strategies and adopt cutting-edge technology to execute the most profitable attacks possible against online merchants. With [Sift Digital Trust & Safety](#), online businesses can quickly implement scalable fraud prevention strategies that don't limit growth for the sake of protection. Using patented, real-time machine learning and over 70B events per month from our merchant data network, Sift proactively detects multiple types of abuse spawning from the Fraud Economy, enabling merchants

to refine, scale, and streamline their trust and safety operations with every transaction—and every intercepted attack.

Stay tuned for our next Digital Trust & Safety Index report to explore new online merchant and consumer data, developing e-commerce fraud trends, and expert insights. You can also access any of our 2020 reports [on our website](#).



## About Sift

**Sift is the leader in Digital Trust & Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk.** Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of 70 billion events per month, and a commitment to long-term customer partnerships. Global brands such as Twitter, Airbnb, and Twilio rely on Sift to gain competitive advantage in their markets. Visit us at [sift.com](#) and follow us on Twitter [@GetSift](#).

## Sources

1. Adage, "Rise Of Buy Now, Pay Later Brands Sparks New Lending Industry Marketing Battle." <https://adage.com/article/cmo-strategy/rise-buy-now-pay-later-brands-sparks-new-lending-industry-marketing-battle/2320391>
2. AtlasVPN, "Cybercrime cost the world over \$1 trillion in 2020." <https://atlasvpn.com/blog/cybercrime-cost-the-world-over-1-trillion-usd-in-2020>
3. Forbes, "COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal." <https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=1>
4. U.S. Census Bureau, "Advance Monthly Retail Trade Report." <https://www.census.gov/retail/index.html>
5. Blackbaud Institute, "Online Giving Trends." <https://institute.blackbaud.com/charitable-giving-report/online-giving-trends/>
6. Sift, "2020 E-commerce Fraud Data: Digital Trust & Safety Index Recap." <https://blog.sift.com/2021/2020-e-commerce-fraud-data-digital-trust-safety-index-recap/>
7. Dark Reading, "New Fraud Ring "Bargain Bear" Brings Sophistication to Online Crime." <https://www.darkreading.com/vulnerabilities---threats/new-fraud-ring--bargain-bear--brings-sophistication-to-online-crime/d/d-id/1338303>
8. Google, "Online Security Survey Google/Harris Poll February 2019." [https://services.google.com/fh/files/blogs/google\\_security\\_infographic.pdf](https://services.google.com/fh/files/blogs/google_security_infographic.pdf)
9. Business Insider, "Rise of M-Commerce: Mobile Ecommerce Shopping Stats & Trends in 2021." <https://www.businessinsider.com/mobile-commerce-shopping-trends-stats>
10. FastCompany, "Report: Scammers will offer you cheap food delivery on Telegram, then pay for it with stolen credit cards." <https://www.fastcompany.com/90603698/report-scammers-will-offer-you-cheap-food-delivery-on-telegram-then-pay-for-it-with-stolen-credit-cards>