sift

Q1 2020 DIGITAL TRUST & SAFETY INDEX

A Rapidly-Changing Fraud Landscape

Contents

3 A Rapidly-Changing Fraud Landscape

4 The Current State of Fraud: Payment Fraud Is Exploding, and It's Increasingly Mobile

5 New Verticals Mean New Opportunities for Fraud

7 New Ways to Pay Mean New Ways to Steal

8 Online Payment Fraud by Day in 2019

9 Summer is the Holiday Shopping Season for Fraudsters

11 Mobile-First Web Access Has Ushered in a Ripoff Renaissance

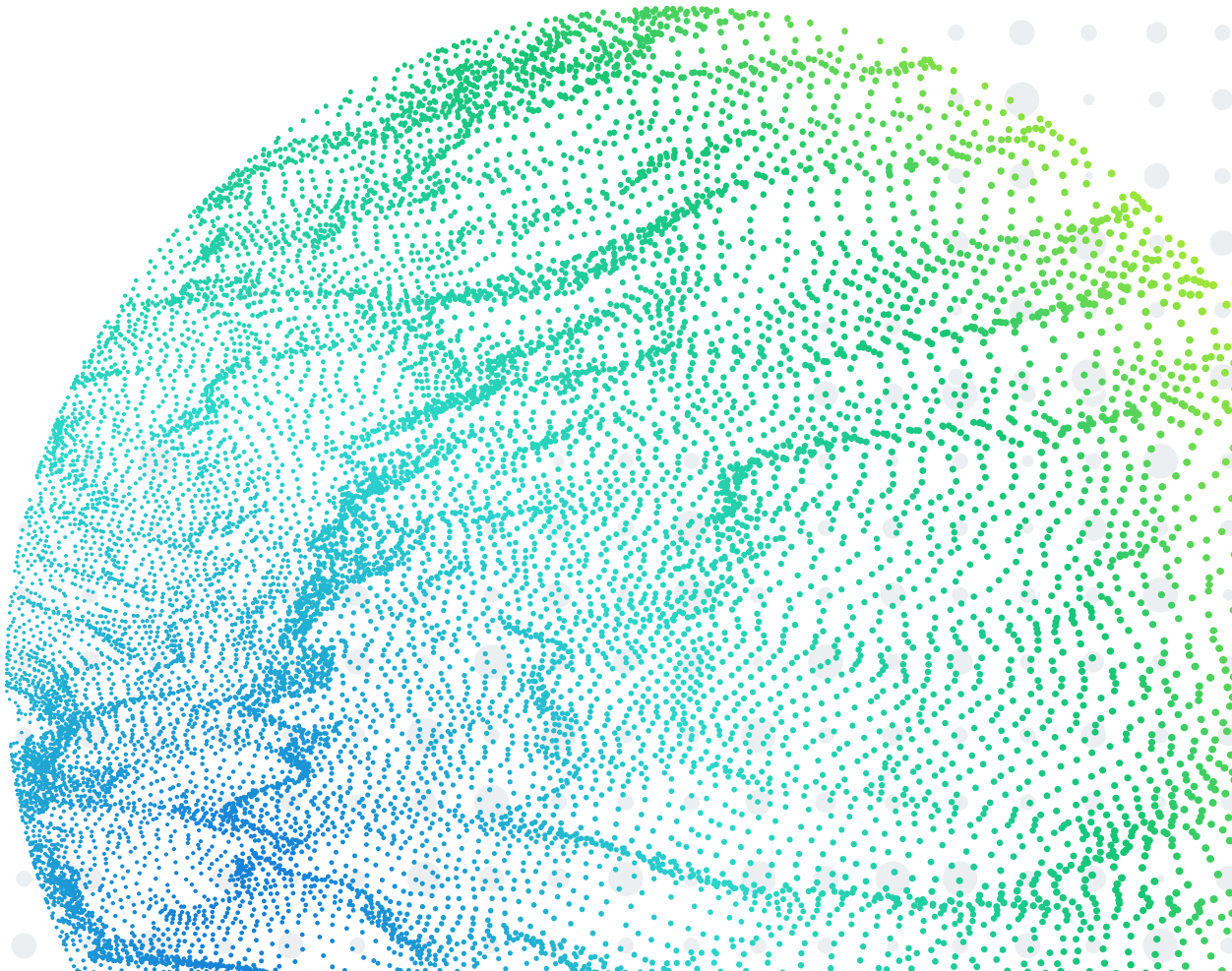
12 Our Understanding of Fraud is Changing — and Trust and Safety Pros Need to Take Notice

A Rapidly-Changing Fraud Landscape

Fraud doesn't stand still. Cybercriminals know that the methods they've used to steal from businesses and consumers in the past will only work for so long — so they change their tactics. Meanwhile, Trust and Safety and fraud management teams chase after these evolving threats by adopting new methodologies and technologies, resulting in a cat-and-mouse game in which businesses must constantly protect themselves against the newest fraud vector.

Our inaugural Digital Trust & Safety Index aims to keep those on the front lines of fraud fighting up-to-date on the latest trends, so they can make informed decisions that will keep their customers and businesses safe from scams, and help them stay one step ahead of fraudsters.

The data in this Index is derived from over 34,000 sites and apps in Sift's customer base. Sift ingests 35 billion events per month to uncover millions of fraudulent events. Our Engineering and Data Science teams derived results by reviewing and analyzing events that occurred across our platform in 2018 and 2019.



THE CURRENT STATE OF FRAUD:

Payment Fraud Is Exploding, and It's Increasingly Mobile

While cybercriminals are finding new ways to defraud businesses and consumers, one classic form of fraud is trending upwards in popularity: payment fraud. Year over year, attempted online payment fraud increased 73% in 2019, well exceeding the growth of digital payments overall. But with one banner year after another of data breaches and compromised payment information, it shouldn't be surprising that we're also seeing an increase in fraudulent payments.

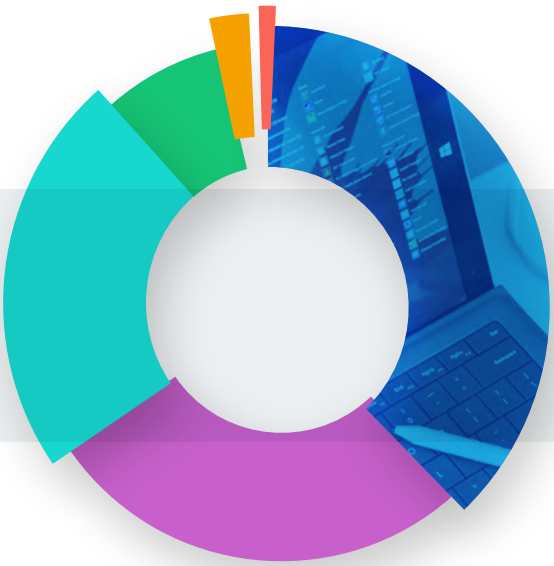
From Marriott to Capital One, to MoviePass and Wawa, hundreds of millions of people saw their credit card and banking information exposed in massive data breaches in 2019. That stolen payment information gets used to commit fraud across the internet, likely leading to the increase in payment fraud that we've seen in the last year.

And notably, fraudsters aren't acting primarily from laptops or desktop computers, but have instead gone mobile: more than half (51%) of the payment fraud attempted in the last year was done via mobile devices, challenging the notion that fraudsters are simply operating in basements on their laptops. For Trust and Safety and fraud teams, this represents a paradigm shift given that only 52% of merchants report tracking fraud on mobile channels. As cybercriminals have taken to these devices to steal from merchants, analyzing mobile signals has become more important than ever to defend against fraud and abuse.

Year over year, attempted online payment fraud in 2019 increased

Attempted Online Payment Fraud by Operating System

Windows: 37.73%
iOS: 27.75%
Android: 22.9%
MacOS: 7.9%
Unix: 2.6%
Other: 1.12%



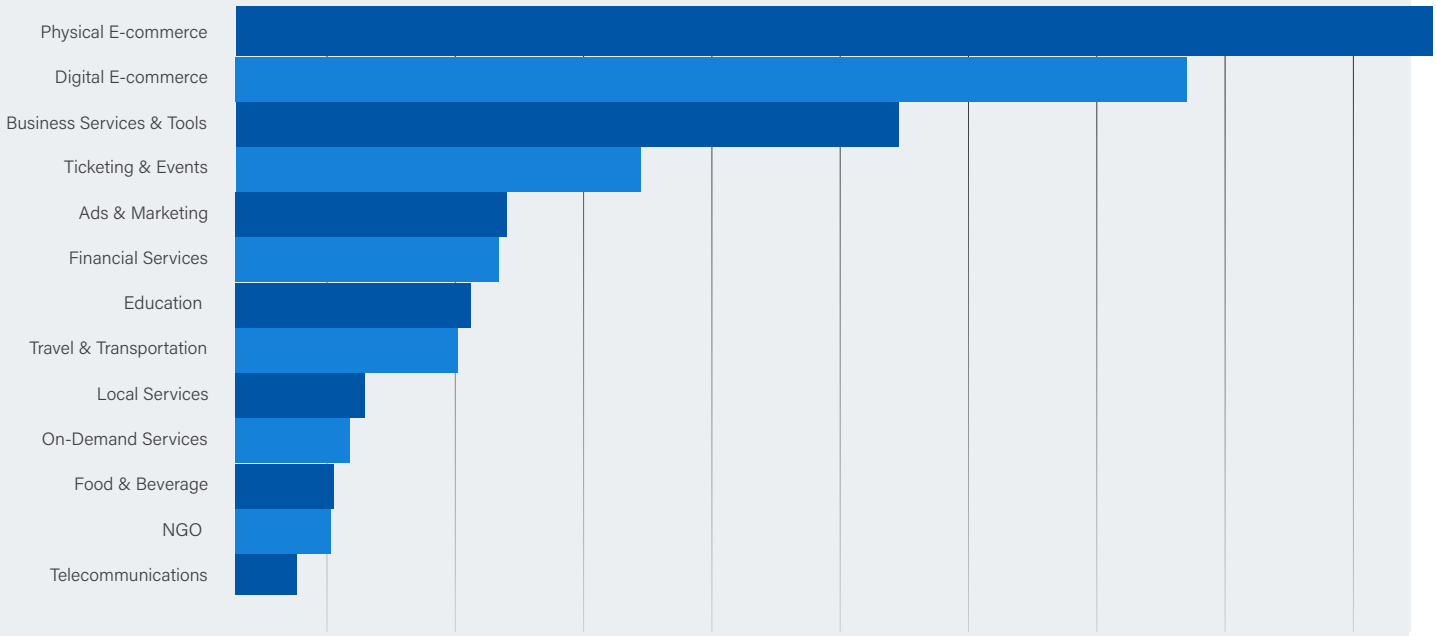
Once fraudsters get their hands on those unwitting users' payment details, Sift looked into their methods and the businesses they target. Our data sheds light on: the verticals hit the hardest by payment fraud, the devices and platforms fraudsters use most, their preferred forms of payment, their preferred times to strike, the most common locations in the world where fraudsters do their work, and other insights.

New Verticals Mean New Opportunities for Fraud

While Physical E-commerce remains the most popular target for payment fraud, Digital E-commerce (often associated with gift cards) has become a highly targeted vertical as well.

1 Physical E-commerce	2 Digital E-commerce	3 Busines Services & Tools	4 Ticketing & Events	5 Ads & Marketing
6 Financial Services	7 Education	8 Travel & Transportation	9 Local Services	10 On-Demand Services

The Top Fraudiest Verticals of 2019 Were:



While some verticals typically associated with fraud are represented on this list, bad actors are finding new types of businesses to exploit, ranging from Business Services (includes shipping services, domain registrars, commerce platforms) and Education (includes online learning platforms) to On-Demand Services (includes ride-share and food delivery). This points to yet another explanation behind the continued increase in payment fraud: as these verticals mature and attract more customers, fraudsters look at them as untapped opportunities.

Trying to Game the System

The largest attempted purchase on Sift's platform in 2019 was for an in-game item for the PC game, *DOTA 2*. The cost of the attempted payment — which took place in an online marketplace — was $1 million, an obvious case of fraud. Video game promos aren't the type of virtual good that would come to mind for most fraud-fighting professionals when considering risk, but that notion is changing as fraudsters are looking for new avenues to exploit.

New Ways to Pay Mean New Ways to Steal

In addition to the emergence of new verticals as destinations for fraud, cybercriminals are also turning to emerging forms of payment that have recently seen a surge in adoption online. The payment types most associated with fraud in 2019 were, in order:

01 Online Promos

02 Digital Wallets

03 Money Orders

04 Cash

05 Cryptocurrency

06 Gift Cards

07 Credit Cards

08 In-App Purchases

09 Other Third-Party Processors

10 Rewards Points

Online Promos, Digital Wallets, and Cryptocurrency — newer payment innovations that are digital-only — are three of the top five payment types most associated with fraud, another indicator that fraudsters are exploiting new technologies in an effort to diversify not just where, but how they can steal from businesses and consumers. In the case of online promos for example, 25% of attempted transactions involving these discounts were fraudulent.

Perhaps most surprising, transactions involving credit cards are now less likely to be fraudulent than other digital-first payment mechanisms — as well as cash. "Pay with cash" options, particularly common in certain on-demand apps, also have a higher rate of fraud than credit cards.

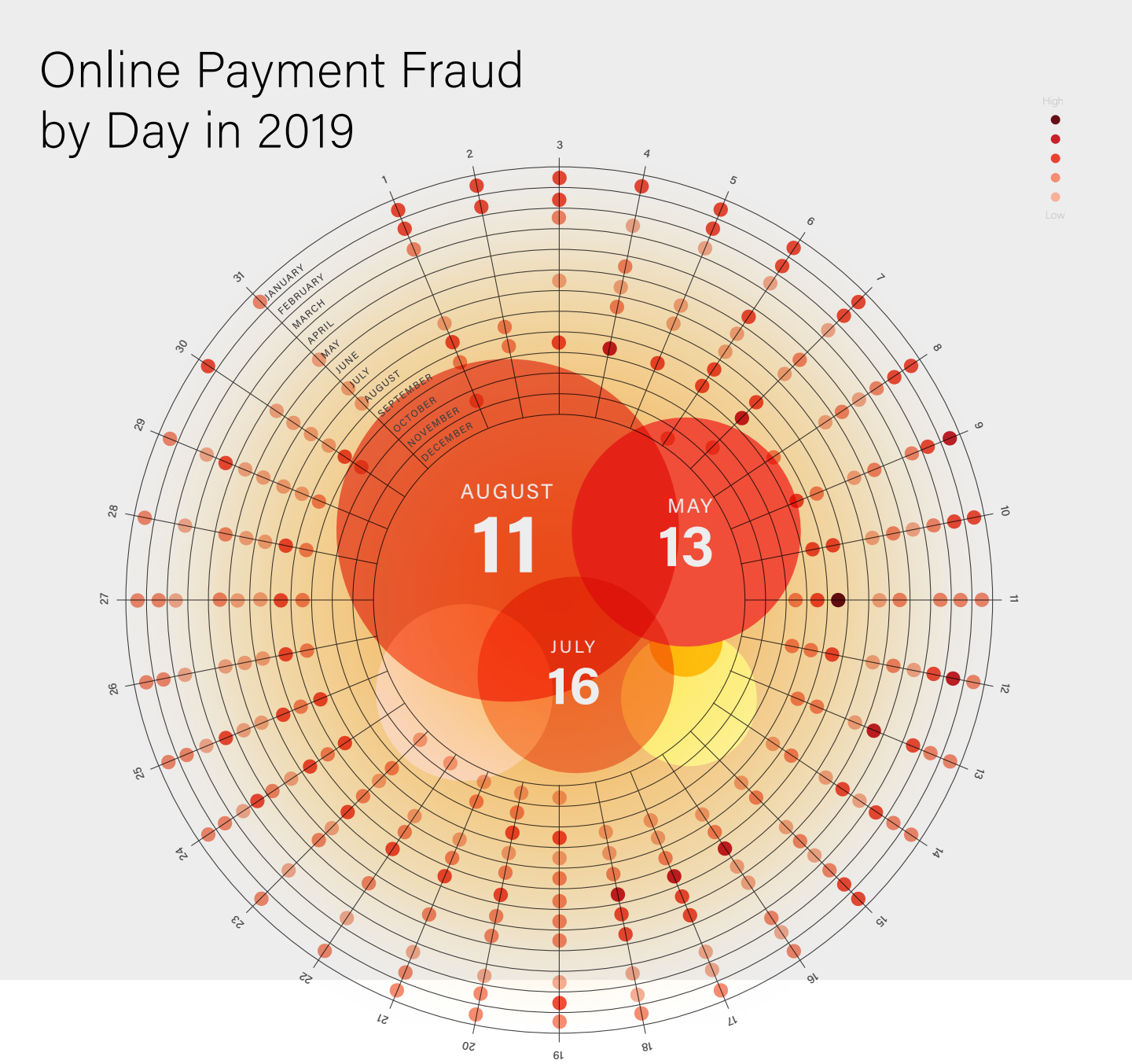
While cybercriminals have been emboldened to steal using different payment types, they are also seeking higher-value scores. Rather than trying to "fly under the radar" by stealing relatively small amounts from a number of businesses, Sift found that the average fraudulent purchase attempt was three times the amount of a legitimate transaction.

While knowing where and how fraudsters commit the most payment fraud is eye-opening, we also have to consider when they're most active in order to stay one step ahead of when they're expected to strike.

Average Fraudulent Purchase Attempt:

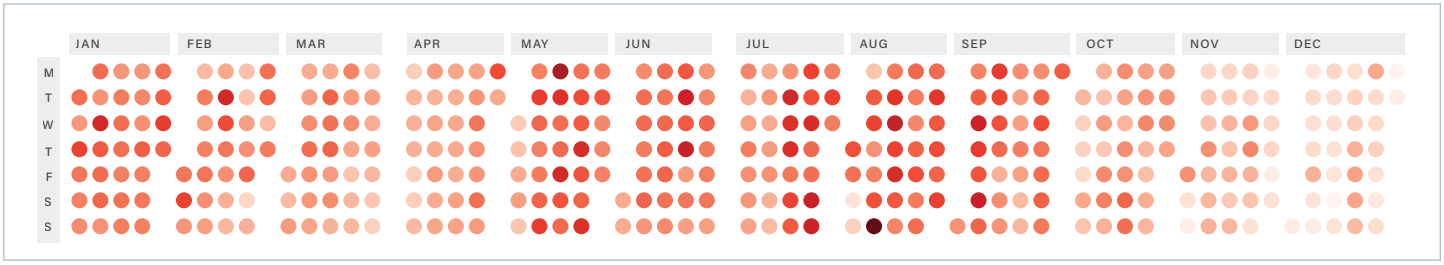
3x

the amount of a legitimate transaction



Overall Fraudiest Days, 2019

Overall, our data shows that August 11th, a Sunday, was the fraudiest day of 2019. The overall fraudiest day of the week was Saturday, highlighting that fraudsters favor the weekends to rip off businesses.



Summer is the Holiday Shopping Season for Fraudsters

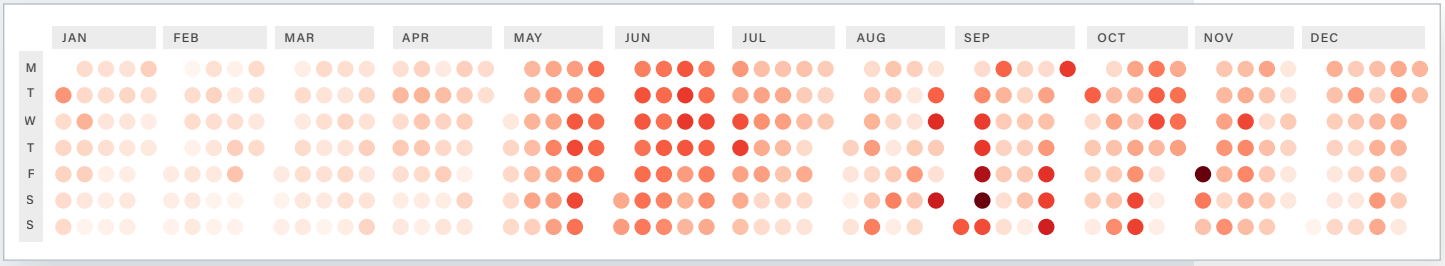
Generally speaking, most people would assume fraud peaks during the winter holiday shopping season, but our findings revealed that fraudsters kick their scams into high gear when we might not expect them to — and when fraud teams aren't necessarily in holiday high-alert mode.

The summer months — not November or December — are the unofficial holiday shopping times for stealing.

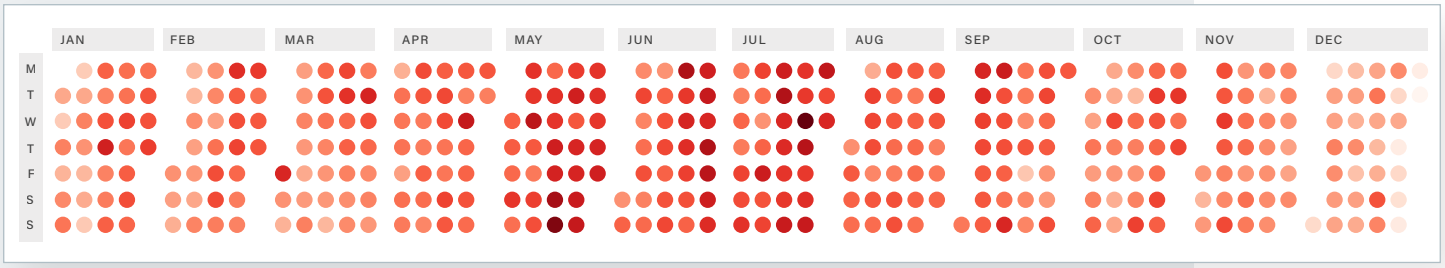
Online Payment Fraud in 2019

Payment fraud in Physical E-commerce starts to heat up in May and June, with greater spikes in September and October. Similarly, Digital E-commerce companies see an increase in payment fraud from May through July, while September is when Financial Services firms experience an increase. Our data illustrates that fraudsters are increasing their efforts outside of what is typically considered the fraudiest time of year, which should be a red flag to fraud and Trust and Safety professionals.

Online Payment Fraud in 2019: Physical E-commerce



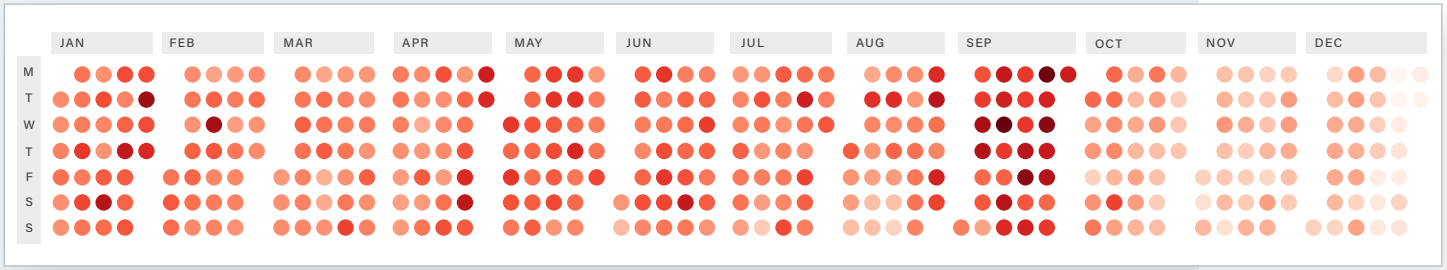
Online Payment Fraud in 2019: Digital E-commerce



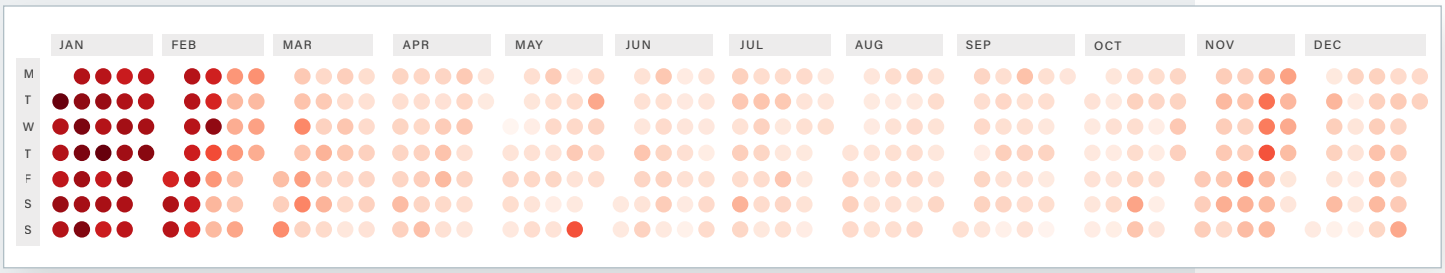
High

Low

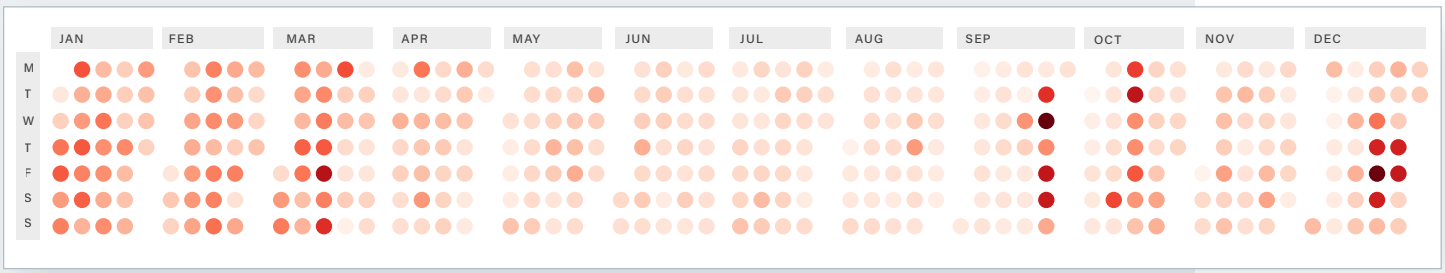
Online Payment Fraud in 2019: Financial Services



Online Payment Fraud in 2019: Travel & Transportation



Online Payment Fraud in 2019: Business Services



Mobile-First Web Access Has Ushered in a Ripoff Renaissance

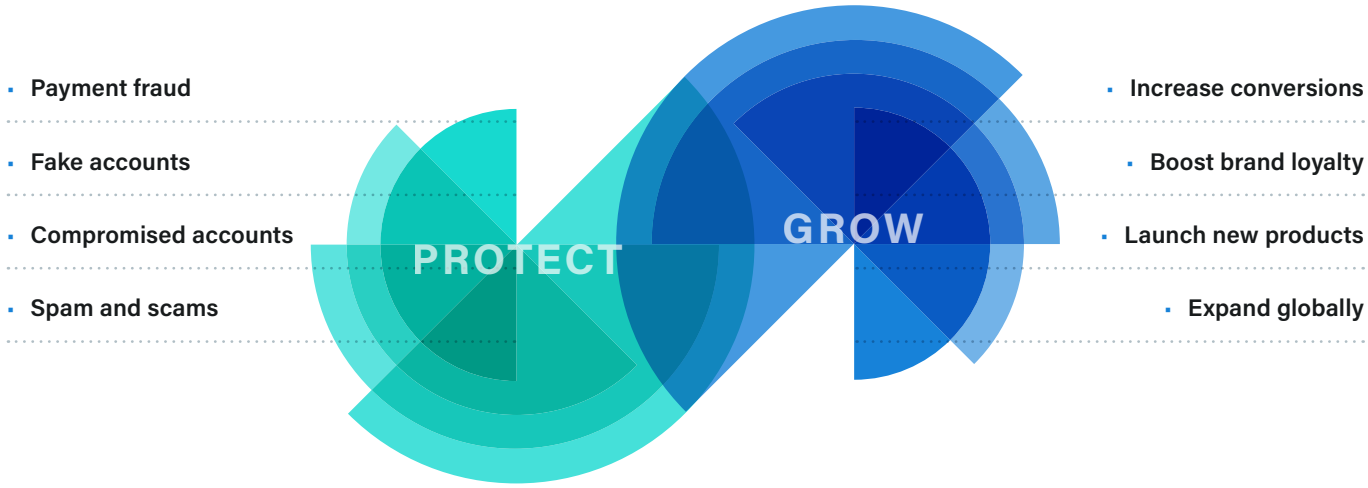
The list of countries most associated with payment fraud gives credence to the aforementioned conclusion: payment fraud has become a mobile enterprise. Internet traffic in most of the countries listed below — including Colombia, Côte d'Ivoire, and Ghana — is primarily or significantly driven through mobile devices. And while the benefits of increased internet penetration in these countries are clear, scammers are taking advantage of mobile web connectivity in order to defraud businesses with stolen or inauthentic payment mechanisms.

Other countries on the list, including Belgium and Mexico, have been previously identified as nations with increasing occurrences of online fraud.

Our Understanding of Fraud is Changing — and Trust and Safety Pros Need to Take Notice

Trust and Safety professionals and frontline fraud fighters are in a constant battle of wits against fraudsters, with both sides working tirelessly to evolve their tactics and methods. Our findings reveal a troubling trend: cybercriminals are exploiting newly emerging technologies and changing behaviors to subvert effective fraud prevention and throw fraud professionals off their scent. Understanding and internalizing these developments is critical in establishing Digital Trust & Safety strategies, which help businesses proactively protect against fraud while reducing friction for legitimate transactions.

As cybercriminals continue to adapt their practices to exploit new technologies, look for our next report to arm you with the information you need to remain one step ahead of bad actors.



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 35 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**.