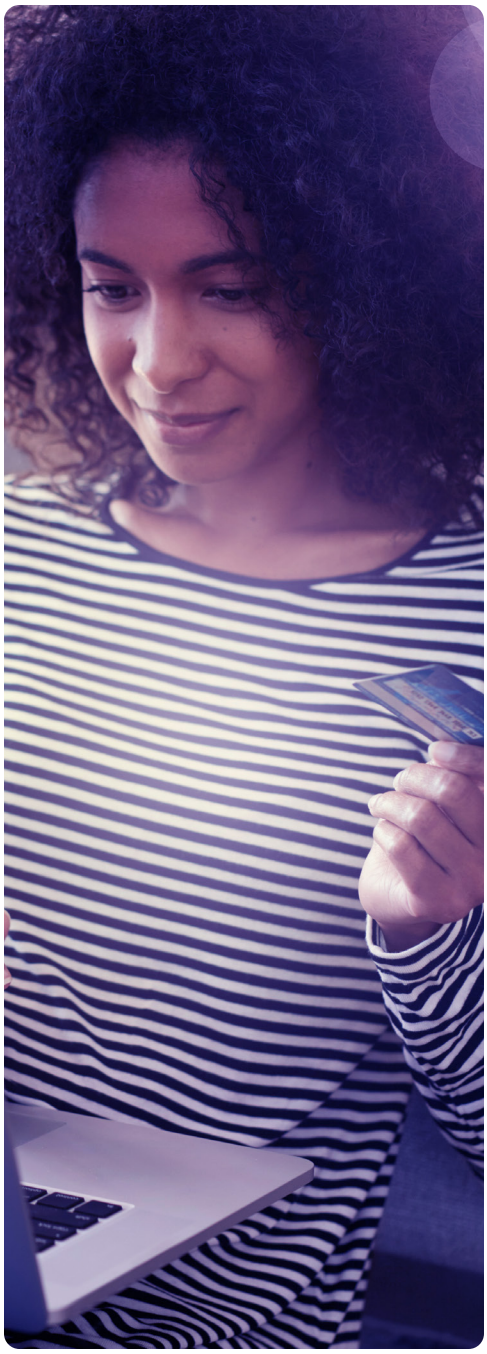


Peak Trading — The Perfect Storm for Fraudsters

ACI Worldwide
Real-Time Payments

Executive Summary

Effective fraud management strategies help increase conversion and protect genuine customer relationships all year round. At peak trading times, however, when volumes spike, consumer behaviors change and pressure mounts on merchant resources. Opportunities increase for fraudsters — and maintaining the right balance between customer experience, sales conversions and risk mitigation becomes even more critical.

1 When Did You Last Review Your Peak Fraud Management Strategy?

Amazon U.K. is reported to have sold around 86 items per second on Black Friday in 2015, and total U.S. online sales (across merchants) on Cyber Monday rose 16 percent from the previous year, to $3.07 billion[1]. There is no question that peak trading days provide major revenue opportunities for eCommerce merchants.

However, the rapid rise in volumes during peak puts increased pressure on all parts of a merchant's business, from the technology infrastructure to payments and security, right through to fulfillment and delivery. Failure to prepare appropriately can lead to cart abandonment, missed revenue opportunities, customer dissatisfaction, increased losses from fraud attacks and damage to brand reputation. Each part of the chain needs to work perfectly — and fraud management strategies have a very important part to play.

2 What Impact Does Peak Have on eCommerce Fraud?

With opportunity comes risk, and fraudsters consider peak trading periods as an opportunity to more easily go undetected. They expect a less rigorous approach to fraud prevention during peak periods and hope that their activities will go unnoticed as transaction volumes spike and delivery windows get smaller. Fraudsters recognize that merchants may relax certain rules or adjust their fraud strategy on certain channels during peak periods to allow more customers through at the checkout.

Nevertheless, the right fraud strategy can enable merchants to have highly successful peak periods — welcoming genuine shoppers and converting them into customers and, ultimately, revenue. Conversely, poorly planned peak fraud strategies risk disappointing genuine customers, pushing them into the arms of competitors, and inviting fraudsters to target their business, resulting in higher chargebacks. While some merchants may consider that a certain increase in fraud is acceptable during peak (to compensate for the significant spike in transactions), this doesn't have to be the case, and it is a strategy that should be adopted with caution. Brand reputation and customer experience are not easily rebuilt. While a business may be able to absorb a short-term, low level of additional costs, other risk factors are not so easily rectified and can have a significant long-term impact on the bottom line.

Before merchants can identify the right fraud strategies, they first need to get aligned internally and understand in detail their own peak trading periods.

3 It's Not All About Black Friday. When Is Your Peak?

Is peak the same for everyone? Should all merchants focus on Black Friday? The short answer is "no" — peak varies. So when is peak?

In the U.K. and North America, Black Friday (the Friday following Thanksgiving in the U.S.), is now one of the most significant peak trading days of the year for both physical and eCommerce merchants — but it isn't peak for everyone. Merchants need to ensure they know exactly when their peak is — and prepare accordingly to drive maximum conversion, securely at the checkout.

Factors that determine peak trading periods include:

- Country or region within which the merchant operates
- Sector or industry
- Seasonality or significant dates
- Product type
- Merchant-specific promotions or sales
- External factors such as exchange rates, regulation and legislative changes

First let's consider the country or region. We have seen explosive growth in Black Friday and Cyber Monday (holiday season) in the U.K. and North America over the last five years and are starting to see the same rapid growth in other European countries.

> **"Fraudsters definitely try to maximize the opportunity peak provides. They take advantage of last minute shopping and smaller delivery windows. They hope their activities will pass undetected in the heightened volume of traffic in attractive, often high-end purchases."**
>
> Craig Jones
> Senior Risk Analyst
> ACI Worldwide

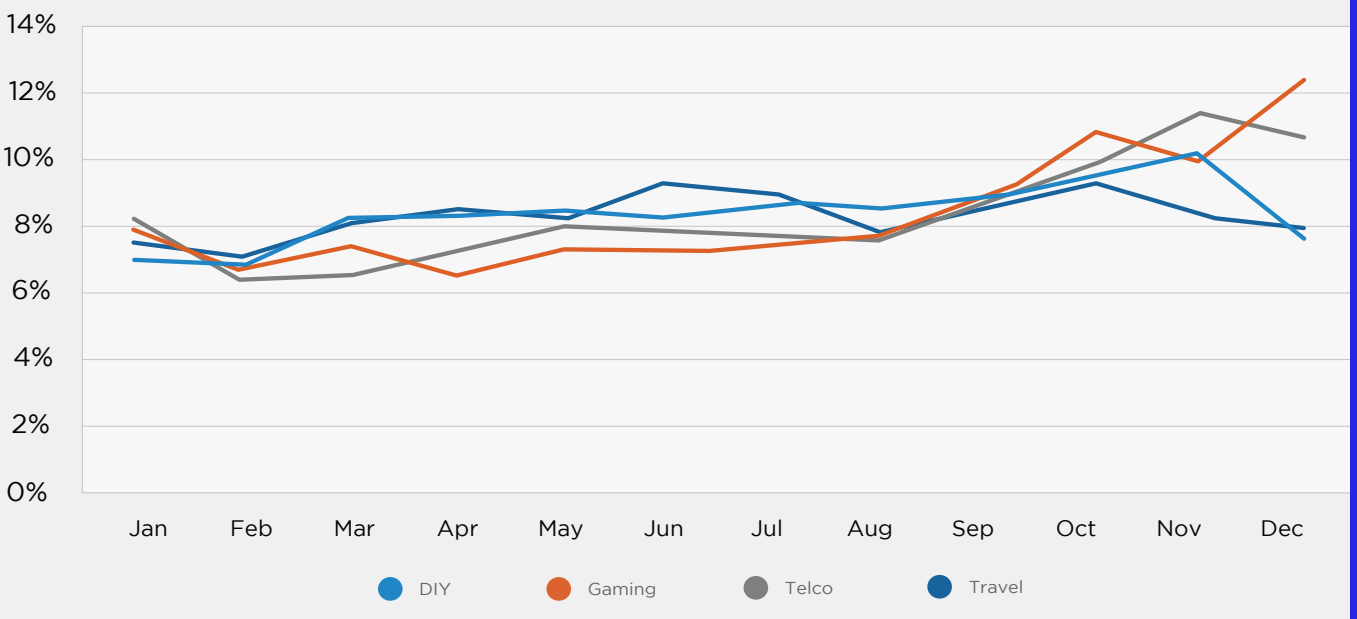
However in China, Singles Day, held on November 11, is now considered to be the busiest online shopping day on the calendar, eclipsing Black Friday and Cyber Monday[2]. Local public holidays and special events can also produce an increase in traffic, as can sporting wins and other significant celebrations.

The industry within which a merchant operates will be another, if not the most significant, trigger for peak periods. Although a number of retail merchants will relate to Black Friday and the pre-Christmas build up, there are merchants in other sectors for whom peak periods vary significantly.

In the travel industry, for example, peak volumes typically occur in the spring months, with people booking their summer holidays. However, there are also peaks in early autumn, as customers plan and book for travel over the Christmas period. The release of blocks of tickets for use over the Christmas period can trigger a mini peak, seen in October, in the graph above. Travel merchants are also more likely to be affected by external triggers such as changes in exchange rates, which can drive mini and unexpected peaks. Real-time fraud strategies need to be implemented for each of these peaks as well as strategies for retrospective screening closer to the time of travel.

Seasonality also affects "Do It Yourself" merchants, who see small peaks in the spring and summer months, in addition to a November peak when they promote Black Friday offers.

Peak Trends - By Industry



ACI Worldwide, 2015. % = % of the year's transactions in that month

Buy online/ pick-up in-store, which has a higher fraud attempt rate than other delivery methods, increased during the holiday season in 2015. At ACI, we saw a 47 percent increase in attempted fraud rates on this channel as well as a 50 percent increase in attempted fraud on next-day and overnight delivery.

The types of products sold relate closely to the industry within which the merchant operates and will trigger peak periods requiring specific fraud management strategies. For digital goods such as games and music downloads, merchants can experience a very significant increase in traffic when new games or high-profile albums are released.

Marketing campaigns clearly drive peak in these industries, in this case increasing pressure on website performance, rather than on physical logistics and delivery. Fraud management strategies for digital download merchants need very close attention as the time from purchase to receipt of goods is virtually immediate, with no opportunity for rescreening, and accept/deny rules need careful consideration. Similarly, in the mobile telecom industry, significant peaks take place when new handsets are launched, again impacting website, payments and delivery logistics. Fraud rules need to be tailored to cater for these specific launches.

Finally, there are other triggers for peak which are completely outside merchant control, with changes in exchange rates, regulation and legislation all capable of rapidly driving up consumer demand.

4 Optimizing Fraud Management Strategies for Peak Periods

Once you have identified your peak trading periods, what can you do to ensure you are well prepared?

A well planned and thought out fraud management strategy can increase revenue by a least 20 percent, so whether you are a retailer planning for Black Friday or a gaming company creating an impactful marketing campaign ahead of your next big launch, we encourage you to consider the following steps for maximum success:

1. Review and prepare your systems

- Deploy automated risk strategies — this can help reduce manual review rates and lower call center operational expenses, helping to control the demand on internal resources.
- Utilize early warning indicators — access to early warning indicators, such as acquirer reported fraud, will help you reduce your exposure and mitigate losses as quickly as possible if under attack.

"A well thought out fraud strategy can increase revenue by at least 20 percent over the industry average."

Erika Dietrich
Director Payments Risk Management
ACI Worldwide

2. Identify your weak points

- How were you compromised last time? Understand where the pitfalls were and tailor your strategies to ensure it doesn't happen again. If delivery fraud was previously a problem, for example, identify the postcodes which need higher review rates and re- focus reviews and resources from areas which pose less risk.
- Consider anything that's changed since the last peak period. What changes have been made to product lines, sales channels, available payment methods and delivery options? Are these new initiatives protected with specific and tailored fraud rules and strategies?

3. Consider the customer experience

- Identify your loyal customers. Customers shop across a variety of channels and touch points. It is important you recognize and enable them, regardless of the device or sales channel they adopt.
- Use customer profiling and time on file techniques to maintain the customer experience for valued customers and ensure good transactions are still accepted — while still being stringent enough to recognize popular methods of attack such as account takeover.

4. Be proactive, understand trends and learn from manual reviews

- Analyze and monitor your fraudulent hot spots and trends. Understand which cards, IP and email addresses pose the biggest threat — ensure you monitor them and factor them into your rules and alert triggers.
- Use all available data. We recommend that you retain one individual to look holistically at data and trends including decisions, individual performances, rules, volumes and KPIs. Remember that manual reviews are still important and every review adds to the wealth of fraud intelligence you can use to inform your decision-making.

IN RECENT YEARS AT ACI, WE HAVE SEEN 78 PERCENT OF FRAUD ATTEMPTS COME FROM CONSUMERS WITH NO ACCOUNT HISTORY WITH A MERCHANT.

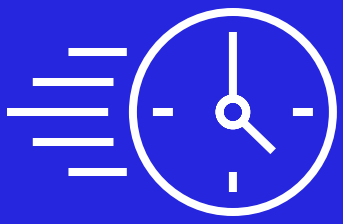
- Be aware of other parts of the payments process that trigger declines — 3D Secure, AVS/CV2 responses and bank declines. How will you manage those, as they can also trigger multiple attempts from customers, compounding the pressure on your website?
- Explore the use of silent rules and reporting tools to screen lower-risk transactions.

5. Communicate with your business

- Talk to colleagues. Cross-functional communication (with IT, finance, customer services and marketing colleagues) can help build a picture of what happened last time — and inform this year's decisions.
- Understand this year's campaigns and promotions. Is your marketing team planning anything that could inadvertently provide opportunities for fraudsters? Ensure you have all the information you need and raise concerns and potential problems. Offer solutions informed by fraud monitoring processes, analytics and reporting.
- Adjust your rules accordingly and in advance, ensuring that they allow for the potential changes in genuine customer buying behavior that may result from campaigns.

6. Continue to monitor and update

- Use your business intelligence tools and real-time monitoring to help make up-to-the-minute decisions and provide faster responses. Don't wait until after peak to see how and where you can improve — keep checking throughout. Use rapid access to fraud intelligence to inform rules changes in real-time.



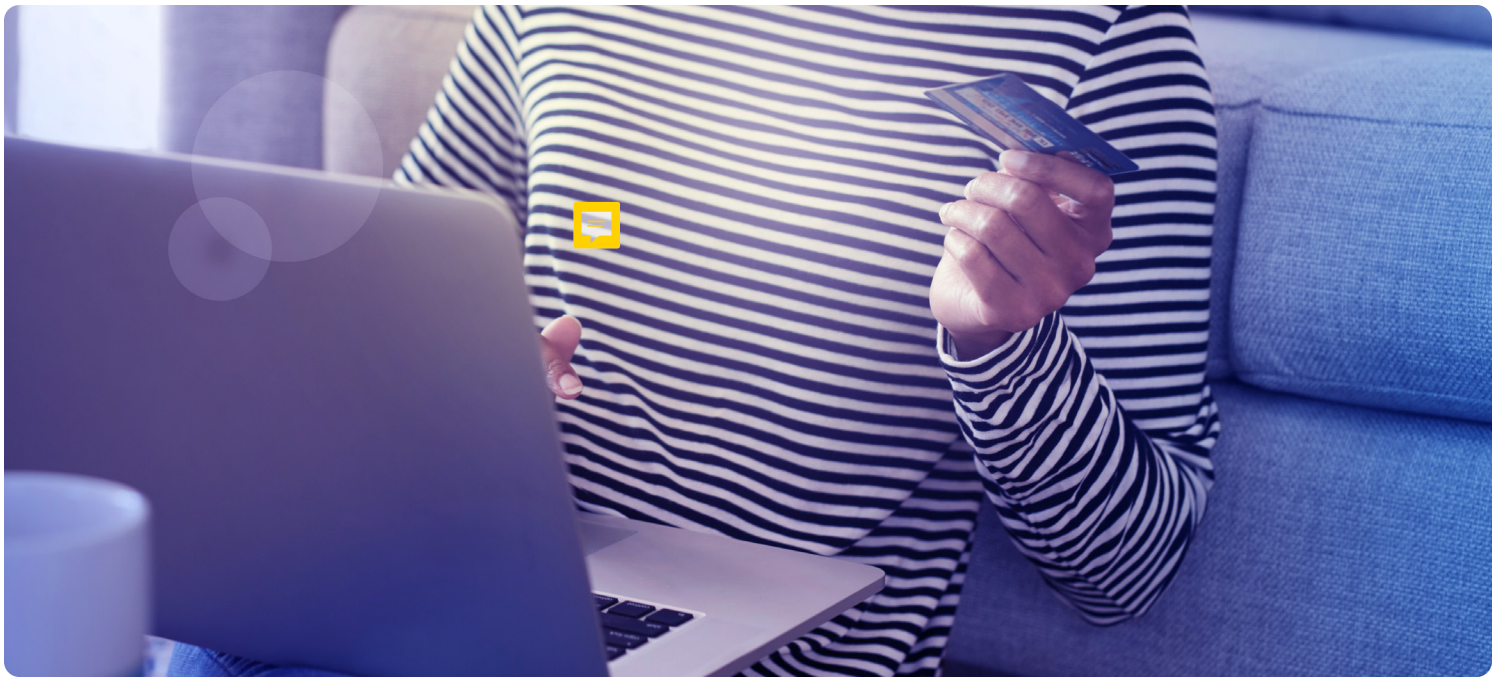
5 Use Your Risk Analyst to Help You Navigate Through the Storm

To enter peak periods in the best possible position, work with experienced risk analysts to review and refine your fraud strategy. Discuss concerns about your fraud rulesets and seek advice on how they should be updated. In this way, you can avoid the storm, deliver a seamless, secure and satisfying shopping experience to your customers and a profitable trading period for your business.

For more information on how to identify and prepare for peak trading, email us at contact@aciworldwide.com.to

[1] https://techcrunch.com/2015/12/01/amazon-dominated- 36-of-online-black-friday-sales-says-slice/

[2] http://www.forbes.com/sites/liyanchen/2015/11/10/ chinas-singles-day-is-already-bigger-than-black-friday- now-its-going-global/#132fd19449da



ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ATL1345 07-21

ACI Worldwide
Real-Time Payments