QUICK GUIDE

BLACK FRIDAY & CYBER MONDAY

29 November 2019
2 December 2019

HIGH CONVERSIONS, LESS FRAUD

Are you prepared for the imminent Black Friday and Cyber Monday? Run a last-minute check now and take the right steps to make the year's highest sales days a success – for you as well as your customers.

TOP 5 FRAUD TYPOLOGIES THAT ONLINE SHOPS FACE

Name & address variations: Fraudsters may use varying names and addresses to subsequently claim that they never received the goods they ordered.

Identity theft: Fraudsters may use an existing name and a third party's address to change the delivery address of the goods later or send the parcel to a drop-off point.

Friendly Fraud: Fraudsters may buy goods, but be unable or unwilling to pay for them.

Account takeover: Fraudsters may acquire customers' online accounts or account data to make purchases, transfer money or obtain even more data.

Return fraud: Fraudsters may return goods, but withhold some of the contents for themselves.

TOP 3 PRINCIPLES OF FRAUD PREVENTION

Although lots of fraudsters are active on these days, you should avoid the mistake of being too restrictive. After all, your loyal customers don't want to be punished for the behaviour of a criminal minority.

1. Be aware of the specific fraud issues you've experienced in the past. Reviewing these incidents can open up new perspectives.
2. Maintain a balance between a pleasant customer journey and a high level of security.
3. The more sophisticated your fraud prevention is, the lower the costs you'll have afterwards.

TOP 8 TIPS FOR YOU

TO KEEP IN MIND FOR A PROFITABLE AND SECURE END YEARS BUSINESS

Social media: Keep an eye on Instagram as well as other platforms and well-known deal websites. This way, you'll always know what's going on in your target market. Setting an alert is more important than ever.

Product groups: Which product groups are especially popular among fraudsters? Which products have low margins and should have fewer restrictions?

Shopping basket limits: Tailor your shopping basket limits according to product groups and segments.

Payment options: Check which payment options are particularly susceptible to fraud and decide which payment methods to allow.

User activities: Have inactive accounts suddenly become active again? Better take a closer look.

Blacklisting: Make sure you bar data from all previous cases of fraud (device, name and certain addresses or areas).

Channels: Which channels do fraudsters use to find you? Consider past risks and decide which channels to place ads on when advertising your shop.

Dispatch: Prevent any subsequent address changes and express deliveries. Both are often exploited by fraud operators.

YOUR LONG-TERM SECURITY PLAN:

Ask yourself how high your internal costs are, to get a handle on your specific fraud issues. Are your activities effective? Can you deal with increasingly sophisticated fraud attempts? Our recommendation is to invest in technology. Consider the following solutions:

SCORING AND IDENTITY
DEVICE TRACKING
VELOCITY CHECKS
(EMAIL, FAKE NAME, ACCOUNT AND DEVICE)

IS YOUR RISK MANAGEMENT PARTNER ALREADY ON BOARD?

DIESE FRAGEN MÜSSEN SIE IHREM PARTNER VOR DEM BLACK FRIDAY & DEM CYBER MONDAY STELLEN

KPIs: Which KPIs are available from previous years?

New approaches in fraud: Has the focus on your specific areas of fraud changed? Are certain types of cases particularly prevalent?

Performance: Request an analysis of your performance. What factors impact on conversion and which affect security?

Limit controls: What shopping basket limits are compatible with your sales targets and desired level of security?

WE WISH YOU A SUCCESSFUL
BLACK FRIDAY & CYBER MONDAY

A service by © Arvato Financial Solutions
finance.arvato.com

Your backbone for growth.