WORLDLINE

Payments to grow your world

Black Month Fraud guide for banks.

How to detect, prevent and communicate about fraud during peak periods.



"**Black Friday**" and the extended "**Black Week**", "**Cyber Month**" or "**Black Month**" periods bring record-breaking transaction volumes and, of course, a corresponding wave of fraud attempts. Fraudsters take advantage of increased consumer urgency and high transaction volumes to exploit vulnerabilities across the payments ecosystem.

This paper outlines the main fraud risks banks face during these periods, the red flags to monitor, and the key measures institutions can take to stay resilient, combining prevention, detection, and customer awareness into one unified strategy.

How much is the world losing to fraud?



- The global e-commerce fraud losses have risen from **$44.3 billion in 2024** to **$107 billion by 2029** ⇒ **a growth of 141%**[1].
- Black Friday period brought online shoppers **over 14,000 cases of fraud in 2023**[2].
- UK-based consumers lost **over £11.5 million** to online criminals between November 2023 and January 2024–with **each victim losing £695** on average[2].
- In Belgium, an increase in AI-fueled fraud cases involving fake bank employees around Black Friday was reported, leading to fraudulent card payments. Overall, fraud has increased by **80%** over the past three years, with identity fraud up **74%**[3].
- During 2024 Black Friday, millennials and Gen Z were **three times more likely** than boomers to be the victims of online shopping fraud[4].
- Europe is targeted by **44%** of all the global Black Friday scams[4].

---

1 Merchant Fraud Prevention Market Report 2024-29: Size, Growth
2 Black Friday warning: shoppers urged to protect themselves... -NCSC.GOV.UK
3 Rising wave of fraud threatens Belgian consumers as Black Friday approaches
4 Black Friday scams: How can shoppers better protect themselves? | Euronews

The risk landscape

November brings more transactions, more customers, and more pressure on fraud systems. The fraud landscape doesn't just grow in volume during Black Month, it changes shape and pattern.

Banks and payment providers typically see five recurring patterns:



Higher volume, lower visibility

Transaction spikes make it harder to spot anomalies in time.



Balancing risk and experience

Customers expect instant payments and refunds, so tightening controls too much can frustrate them.



Evolving tactics

Fraudsters test systems with small "probing" transactions before scaling attacks.



Customer urgency

Shoppers act fast and fall easier for fake websites, phishing, or delivery scams.



Cross-channel exposure

Fraud moves between cards, mobile apps, and online banking — where disconnected systems can't connect the dots.

Common fraud scenarios

Fraud type	Black Month use cases	Impact for banks
Fake or Cloned Online Stores	A wave of fake "Black Friday deal" websites appeared using names close to real retailers. Customers paid with cards issued by several banks — only to discover the stores never existed.	Surge in chargebacks and disputes; banks handle high complaint volumes and potential reputation risk.
Account Takeover	During Cyber Week, fraudsters launched phishing emails pretending to be parcel delivery updates. Many bank customers entered their online banking details, allowing unauthorized transfers and online purchases.	Customer funds stolen, account recovery workload increases, loss of trust in digital channels.
Friendly Fraud	After Black Friday, customers contacted their banks claiming they didn't make certain purchases. Investigations showed most were legitimate transactions such as forgotten orders, delayed deliveries, or buyer's "regret".	Increased dispute processing and chargeback costs; false fraud claims inflate operational workload.
Synthetic Identities	In the weeks before Black Friday, fraudsters created fake identities mixing real IDs with false data. These passed onboarding checks, obtained credit cards, and maxed out limits during sales, then disappeared.	Credit losses and compliance exposure; banks bear the cost of unpaid loans or cards.
Refund / Promotion Abuse	Fraudsters bought expensive items using multiple discount codes, then returned fake packages or claimed false cashback refunds. Some collaborated with dishonest merchants to process fake refunds.	Refund and reconciliation anomalies; potential merchant risk exposure for acquirers.



How banks can respond

Banks are under pressure to process record transaction volumes without slowing down customer experience, but also to protect against a wave of new fraud tactics. The most resilient banks are those that act early, adapt quickly, and connect intelligence across the entire customer journey.

Strengthen real-time visibility
Connect fraud signals across all channels — card, online banking, mobile app, and merchant acquiring — to detect patterns that single systems can't see.

Strengthen readiness before peak season
Identify likely fraud scenarios early and ensure monitoring and escalation processes are in place before transaction volumes surge.

Increase adaptive authentication
Use step-up verification dynamically based on risk signals (new device, unusual IP, high transaction value), not just static thresholds.

Coordinate across teams
Fraud, risk, operations, and communications teams should share one playbook — ensuring faster response, consistent messaging, and smoother customer handling.

Educate and engage customers
Proactive communication reduces fraud. Use in-app messages or short awareness campaigns to remind customers how to identify phishing and fake stores.

Monitor refund and dispute activity in real time
Fraudulent refund or chargeback patterns often appear days after the event — build monitoring dashboards that track anomalies beyond the campaign period.

Communicating about fraud

Fraud prevention doesn't end with technology, it also depends on how banks communicate with their customers and the market. Clear, consistent communication builds trust, reduces panic, and helps customers make safer decisions.

Be proactive

Share short, clear messages before and during Black Month reminding customers how to identify fake offers or phishing links.

Keep it simple

Avoid technical language and focus on what customers can recognize and do.

Leverage digital channels
Use in-app banners, push notifications, or email alerts for quick, targeted updates.

Show empathy, not fear
Reassure customers that security is a partnership: the bank protects them, but awareness protects both sides.

Use data to lead

Publish periodic insights (without revealing sensitive data) to position the bank as a risk-aware, responsible institution.



How can Worldline help?

Worldline is the chosen partner of numerous banks in the European ecosystem for securing their entire payment rails against fraud, not just during this period, but throughout the year.

What makes Worldline the best choice for banks and financial institutions?

Our end-to-end solution, combined with a great concern for a smooth user experience and optimized banking performance.

Scan the QR code to read more about our solution.

About Worldline

Worldline [Euronext: WLN] is Europe's leading operator of critical infrastructure and payment services. With a presence across the entire value chain, the Group offers its customers unique expertise in processing and securing their payments, thereby promoting their growth. Worldline is leveraging its 2030 strategic plan and its technological innovation capabilities to build the European reference payment partner for merchants and financial institutions. With over 1.2 million customers, Worldline achieved €4bn in revenue in 2025. **worldline.com**

For further information
sales-fs@worldline.com

Worldline is a registered trademark of Worldline SA. November 2026
© 2026 Worldline.