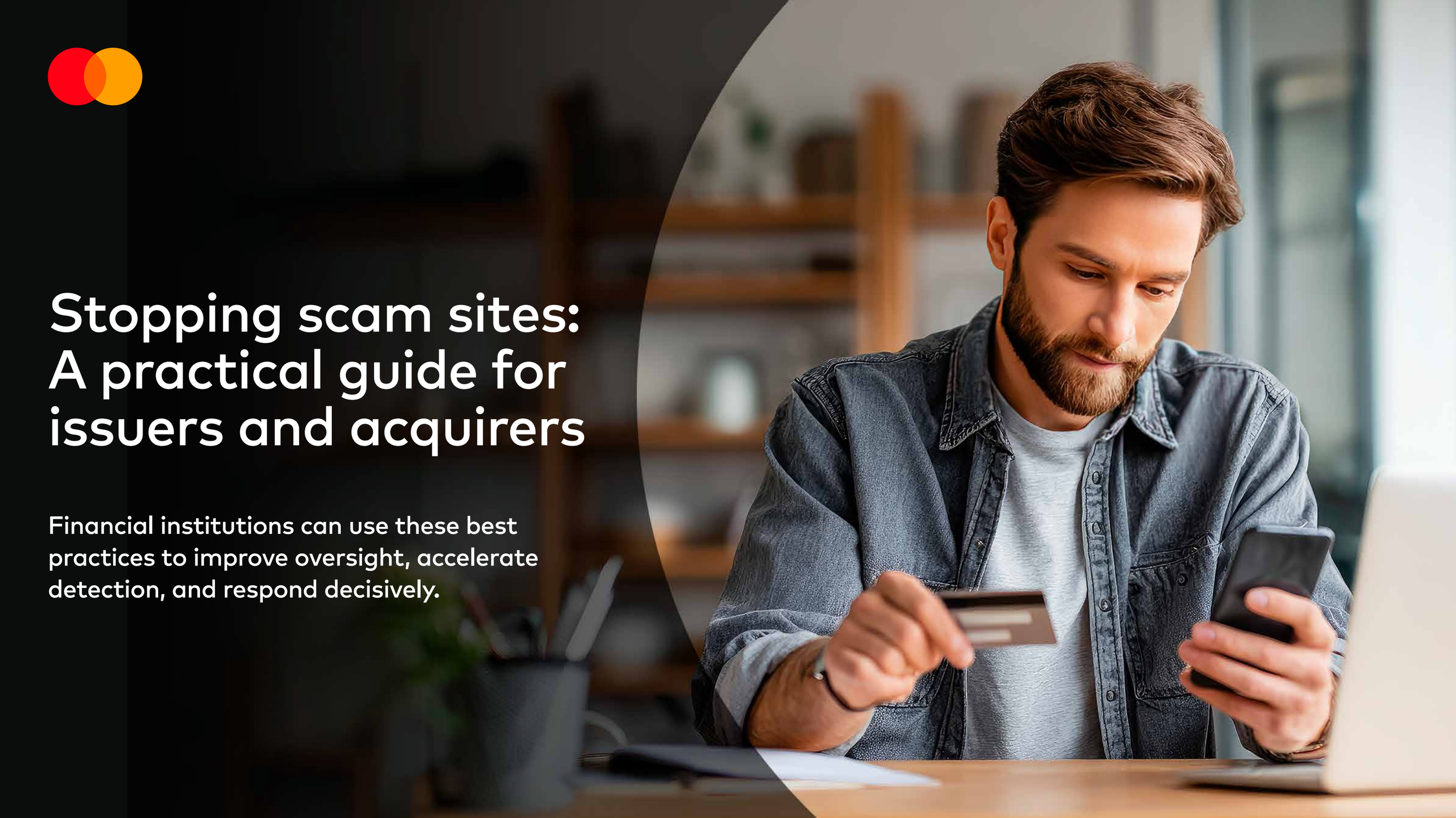
Stopping scam sites: A practical guide for issuers and acquirers

Financial institutions can use these best practices to improve oversight, accelerate detection, and respond decisively.



Global scams surge: Take these steps to protect your business

Scammers stole over $442 billion globally last year, according to the "Global State of Scams 2025 Report" by the Global Anti-Scam Alliance and Feedzai. These attacks exploit consumer trust, trigger costly chargebacks and leave issuers and acquirers to manage the fallout.

This guide delivers practical steps to help stakeholders respond faster, act smarter, and prevent scam activity before it escalates.

57%

of adults globally claim to have had a scam experience in the last 12 months*

Among this group,

54%

reported shopping scams as the most common type of scam experienced*

74%

of adults globally scammed reported the scam to the payment service*

*Source: "Global State of Scams 2025 Report"

Best practices for acquirers

Acquirers help protect the payments ecosystem by ensuring only legitimate, compliant merchants are onboarded. By following Mastercard Security Rules & Procedures and using strong underwriting, monitoring and education, acquirers reduce the risk of working with fraudulent merchants. Here are strategies for acquirers:

Underwriting and merchant due diligence

1. Enhanced due diligence

Verify the merchant's business model, historical payment processing activity and beneficial ownership. Confirm that contact details and corporate information are legitimate and consistent across public sources.

2. Leverage merchant alert and screening systems

Use available industry merchant alert databases, such as MATCH Pro, or others such as Onboard Risk Check, to determine whether a prospective merchant has been previously terminated for non-compliance, fraud or excessive chargebacks. Regular checks may prevent the re-onboarding of known bad actors.

3. Ongoing website reviews

Periodically review newer merchant websites or apps to confirm they align with the information provided during underwriting (for example, product offerings, terms and conditions, and branding).

4. Specialty merchants and high-risk merchant category codes

Verify that the merchant's category code matches the type of goods or services it provides. Monitor for high-risk MCCs, such as illegal gambling or adult content, where additional controls and specialty merchant registration is required.

Transaction monitoring

5. Transaction pattern analysis

Implement real-time monitoring tools that track abnormal spikes, suspicious refund patterns or inconsistent average ticket sizes.

6. Oversight of payment facilitators and sub-merchants

Large-scale scams often exploit payment facilitators managing many sub-merchants across numerous URLs. Acquirers should ensure that payment facilitators:

- Conduct thorough onboarding and URL monitoring using web crawlers, merchant monitoring service providers, and tools that track adverse media and web traffic flows.
- Limit the number of active URLs a sub-merchant can use, ideally to a maximum of three.
- Assign a unique merchant ID to each sub-merchant for traceability and authentication.

Chargeback and fraud management

7. Chargeback and fraud monitoring programs

Acquirers should align their oversight with established chargeback and fraud monitoring programs, such as Mastercard's Acquirer Chargeback Monitoring Program, to identify merchants who exceed chargeback thresholds. When a merchant is flagged, initiate immediate corrective measures such as targeted reviews or hold back reserves to mitigate future potential losses.

8. Collaborative fraud alert tools

Leverage real-time alerts, such as Ethoca Alerts, and data sharing platforms when disputes or suspected fraud occur. Early collaboration can help resolve cardholder concerns before they escalate into chargebacks, helping to reduce dispute volume and financial losses.

Communication, training and escalation

9. Shared fraud intelligence

Maintain direct communication channels with issuers to exchange data on emerging scams or questionable transaction activity. Mastercard encourages all stakeholders to participate in industry consortiums and working groups that address evolving fraud patterns.

10. Awareness and training

Provide merchants with guides on PCI-DSS requirements, dispute resolution and fraudulent indicators. Fraudsters often use incomplete or suspicious details — random names, free email domains or mismatched contacts — to place fraudulent orders. They may also create multiple accounts with slight variations (similar email addresses or shared phone numbers, for example) to avoid detection and carry out repeat scams.

11. Incident escalation plans

Develop clear escalation protocols for suspected scam websites, including immediate risk reviews, site take-down coordination and law enforcement referral procedures. Document findings and share relevant intelligence with Mastercard to aid broader ecosystem protection.

12. Business review sessions

Offer periodic check-ins or webinars on compliance updates, particularly when there are revisions to the Mastercard publications and relevant bulletin announcements.

13. Transparency and consequences

Clearly communicate that merchants engaging in prohibited activities or excessive fraud are subject to account termination, fines or industry reporting mechanisms.

Best practices for issuers

Issuers play a critical role in protecting cardholders and reducing exposure to fraudulent transactions. The following measures help identify and mitigate fraudulent merchant activity early:

Detection and authorization controls

1. Real-time fraud detection

Use AI and machine learning to identify unusual cardholder or merchant activity. Immediate alerts to cardholders can speed up the detection of threats by analyzing transaction velocity, geolocation anomalies and historical purchase behaviors, helping mitigate losses.

2. Dynamic authorization controls

Tailor authorization parameters based on cardholder profiles and risk factors, declining or flagging high-risk transactions in real time. Adaptive risk scoring, based on transaction location, merchant category and historic spending patterns, minimizes friction for legitimate transactions while catching unusual activity earlier.

Dispute and collaboration

3. Accelerated dispute resolution

Issuers should leverage collaborative tools, such as Ethoca Alerts, that alert merchants quickly when a cardholder disputes a transaction as fraud. This can help deflect disputes quickly before the costly and time-consuming chargeback process even begins.

4. Coordinated fraud response

If an issuer is approached by an acquirer with a high impact/critical fraud management request, it should collaborate with the acquirer to the best of its ability.

Cardholder awareness and support

5. Proactive Cardholder Communication

Notify cardholders of irregular spending patterns via SMS, email or app notifications to confirm suspicious transactions quickly and help reduce fraud exposure. Encouraging cardholders to report potential scams promptly prevents further unauthorized transactions and helps issuers obtain metrics to refine risk models.

6. Education and empowerment

Regularly provide content that instructs cardholders on how to spot scams, secure their personal data and report questionable charges immediately. Up-to-date educational materials shared via emails, social media channels or in-app alerts help keep cardholders informed about evolving scam tactics.

7. Overcoming embarrassment and stigma

Some cardholders feel embarrassed after falling for scams that seem obvious in hindsight. This can delay reporting and dispute filing. Issuers can help by:

- **Creating a supportive environment:** Explain that scams are sophisticated and anyone can be deceived.
- **Dedicated hotlines or points of contact:** Offer confidential, empathetic ways to report incidents.
- **Regular awareness campaigns:** Run campaigns stressing that fast reporting can help contain fraud and recover funds.

LEARN MORE

Staying ahead of scam website threats

Scam websites are evolving fast — and so must our defenses. Issuers and acquirers play a critical role in protecting cardholders and preserving trust in digital commerce. Use these best practices to improve oversight, accelerate detection and respond decisively.

Mastercard offers a breadth of capabilities to provide insights for secure authentication, efficient onboarding and help ensure safe and secure transactions. Our Scam Protect initiative provides a three-pronged framework leveraging advanced technology, industry collaboration and education to combat scams.

Learn more in our white paper "Building digital trust by combating scam websites and fraudulent activities".