pwc

Rethinking e-commerce fraud

Strategies for legal and compliance teams

Forensics Today
PwC perspectives on
the newest risks drawing
investigator scrutiny

- E-commerce fraud is growing and becoming harder to detect with bad actors using GenAI, deepfakes and personal data acquired from the dark web to conduct more convincing identity theft and social engineering tactics at scale.
- The consequences for retailers and other e-commerce brands can be serious: class actions, enforcement and fines, not to mention operational disruption, financial losses and reputational damage.
- To help manage this risk, legal and compliance leaders should adapt their strategies, work with first-line counterparts to set risk thresholds, align controls with evolving laws and fraud schemes, and guide the response when thresholds are breached — without creating more friction for customers.

Since the pandemic, the digital commerce landscape has changed dramatically. More consumers, more payment methods, more automation — and more openings for fraud. Criminals aren't just targeting checkout, they're hitting multiple steps across the customer life cycle, including fake sign-ups, account takeover at login, promotional abuse, fraudulent returns and chargeback manipulation.

Armed with new tools, fraudsters are becoming more proficient and sophisticated. GenAI and deepfakes, combined with personal data found readily on the dark web, are enabling them to impersonate customers and businesses with alarming credibility, eluding verification systems with ease. These tools also make ongoing fraud schemes harder to detect, allowing them to continue unchecked for longer periods.

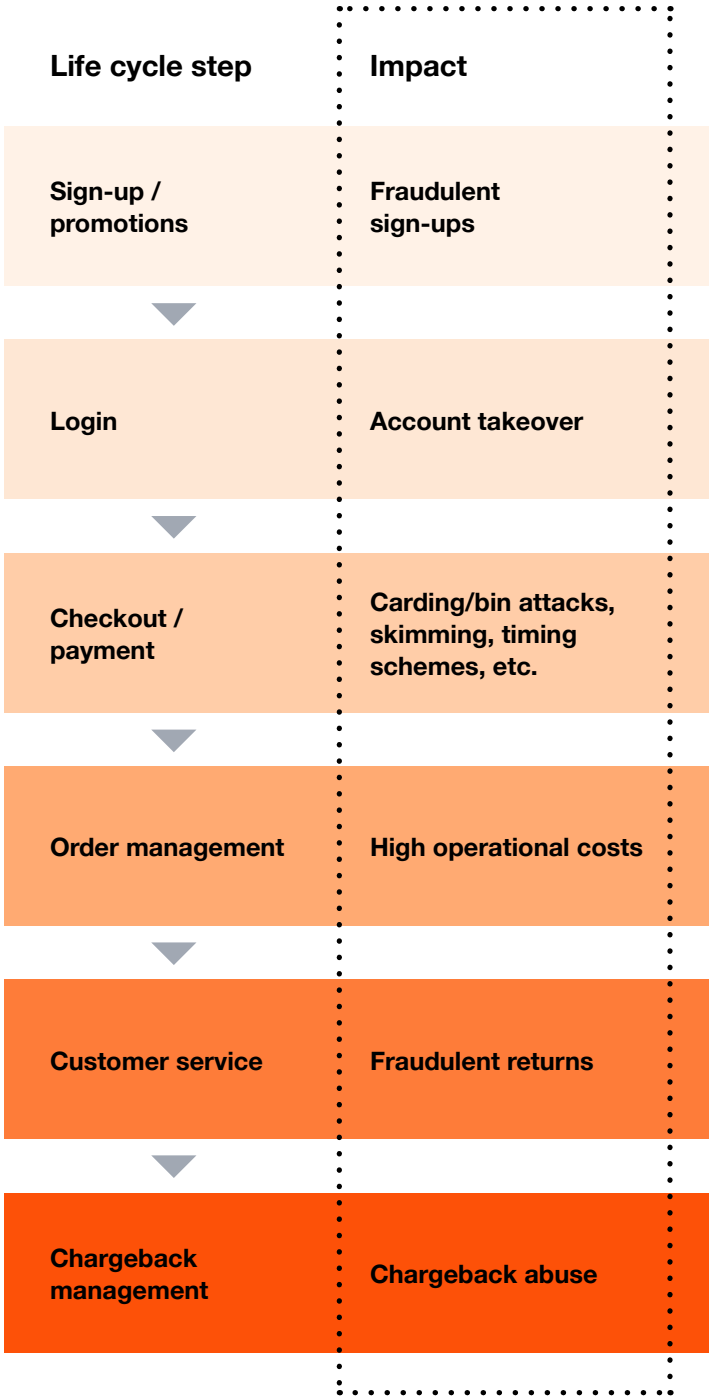
> "While the fraud schemes aren't new, AI is fundamentally changing how criminals carry them out."

Leo Tsao
Partner, Paul Hastings LLP

For many companies in this space, this often means greater legal and regulatory risk. Failure to prevent or mitigate fraud can lead to investigations, enforcement, fines, class actions and loss of access to card networks, not to mention operational disruption and financial losses. All of this carries the potential for serious reputational and brand damage.

Adopting effective strategies for managing this growing risk means fostering better coordination between first-line business leaders and their counterparts in legal and compliance. It also means recognizing that fraud can't be eliminated entirely, only managed — ideally in a way that doesn't hurt the overall customer experience. To that end, general counsel should help the business in setting fraud tolerance levels, aligning controls with legal expectations and guiding the business response when thresholds are breached.

Fraud throughout the e-commerce life cycle



Evolving legal and regulatory complexity

Fraud doesn't happen in isolation, and neither does your response. Every decision you make about fraud strategy, customer experience or risk tolerance plays out against a backdrop of regulatory requirements, cross-border complexity and AI-related risks.

Understanding how fraud risk intersects with privacy, consumer protection, AI and financial regulation is essential for creating controls aligned with those requirements.

You're navigating a growing body of local, state, federal and global regulations that govern how you should collect, store, share and protect customer data — and how you should respond when fraud strikes.

Payment card fraud liability

Payment card fraud liability is a multifaceted legal and commercial issue because responsibility is distributed across merchants, consumers, and card issuers governed by laws, regulations, network rules and other agreements.

Consumers are generally insulated from direct financial loss by the Truth in Lending Act and Regulations Z and E, and by network rules, provided they report fraud in a timely manner. Card issuers typically bear the initial burden of reimbursement but can recover losses from merchants for card-not-present losses.

Payment networks set and enforce the liability allocation regimes (for example, the EMV liability shift or rules governing authentication protocols like 3-D Secure), which can override these expectations and impose obligations that extend beyond local statutory protections. To protect the network from fraud, networks monitor chargebacks and frauds and can enforce significant penalties on merchants with chargebacks and/or fraud losses that exceed the network-defined limits.

For merchants and their legal counsel, navigating this landscape requires careful attention not only to consumer protection laws but also to evolving network mandates and the contractual terms embedded in acquirer agreements, which collectively determine where liability ultimately rests.

Consumer protection compliance

E-commerce merchants that provide financial products (e.g., pre-paid cards or acting as an agent for initiating a wire) or that offer a marketplace can face risk of fraud that creates consumer protection exposure.

Bias and unfairness in AI models have become areas of increased regulatory focus, particularly around compliance with privacy and anti-discrimination laws.

Scammers may deceive consumers into sending them payments or instruments. From a consumer protection compliance perspective, scams create significant legal exposure for merchants because regulators increasingly view the failure to prevent or warn against scams as an unfair or deceptive practice. Under the FTC Act and parallel state consumer fraud statutes, businesses are obligated to confirm their practices don't mislead or harm consumers, even indirectly.

This means merchants must carefully review their transaction flows, disclosures, and customer communications to verify they're not enabling or overlooking scam-related risks. Practically, this translates into obligations around truthful advertising, effective consumer warnings (e.g., for products such as gift cards), and fair dispute handling. Failure to meet these standards can lead not only to regulatory enforcement and penalties, but also to reputational harm, as merchants may be portrayed as complicit in allowing scams to proliferate.

Consumer lending compliance

Merchants that offer payment plans on credit, such as mobile network operators, must comply with the Fair Credit Reporting Act (FCRA) when making credit determinations. They must, for example, have a program to look for identity theft red flags under the "red flags rule" in the Fair and Accurate Credit Transactions Act (FACTA), to avoid targeting legitimate consumers who are the victim of identity theft.

Financial crime compliance

Globally, anti-money laundering (AML) and know your customer (KYC) frameworks continue to evolve, placing pressure on merchants offering payment products and digital wallets, agents of money services businesses (MSBs), and buyer-seller marketplaces in some jurisdictions to strengthen identity verification practices and monitor for financial crimes in real time.

AI compliance

AI and automated decision-making tools are reshaping the fight against fraud, but they also introduce new legal uncertainties. Bias and unfairness in AI models have become areas of increased regulatory focus, particularly around compliance with privacy and anti-discrimination laws. This has prompted a broader shift toward **Responsible AI**, the practice of designing and deploying AI systems that are fair, transparent, accountable and aligned with legal and ethical standards.

Many regulators are beginning to ask how automated systems make decisions, prompting expectations for explainability, auditability and human oversight. For example, if an AI-system incorrectly flags a legitimate transaction as fraudulent, your organization may face government scrutiny, as well as potential liability for negligence, discrimination or breach of contract. The Department of Justice has issued **updated guidance** stating that it expects companies to take steps to evaluate the risks in their use of AI and adopt adequate measures to manage those risks.

Data and privacy protection

In the United States, laws such as the Federal Trade Commission (FTC) Act, Gramm-Leach-Bliley Act (GLBA) and California Consumer Privacy Act (CCPA) set standards for data protection and disclosure practices, and — particularly in the case of GLBA, which applies to companies offering financial or payment products — include requirements relevant to incident-response planning. In addition, the **Payment Card Industry Data Security Standard** (PCI DSS) sets data security requirements for merchants that store, process or transmit cardholder data.

In recent rulings, the FTC has asserted that consumer-facing digital platforms should offer multi-factor authentication (MFA) on consumer accounts, and that MFA for employee and contractor accounts should be resistant to phishing attacks such as attacks on one-time passcodes (OTP) sent to mobile phones.

In the European Union, the General Data Protection Regulation (GDPR) and Payment Services Directive 2 (PSD2) set even higher bars for transparency, authentication and consumer protection.

Taken together, these mandates form a broad compliance landscape. Understanding how fraud risk intersects with privacy, consumer protection, AI and financial regulation is essential for creating controls aligned with those requirements.

Fraud types with legal exposure

These are some of the more common and legally significant fraud types facing e-commerce business today.

- **Account takeover or loyalty point fraud:** ATO is a growing source for fraud loss if accounts have stored cards attached, digital wallets, loyalty points or other assets of value to fraudsters. Companies are under increasing pressure to demonstrate that they've taken reasonable steps to protect accounts such as offering multi-factor authentication to consumers, monitoring, and other security controls.

- **Identity theft and synthetic identity fraud:** This fast-growing fraud type often targets merchants directly, resulting in financial losses when goods or services are obtained using fictitious identities. While legal prosecution can be complicated by the lack of a traditional "victim," regulators are pressing for stronger KYC/AML standards to prevent synthetic identity abuse in account-based and payment product environments. Additionally, systems for identity verification and fraud monitoring must meet regulatory expectations around processing of personal data involved in identity verification such as IDs, biometrics, or behavioral data. Companies can face liability under GDPR and other data protection laws if they fall short.

- **Friendly fraud or chargeback abuse:** Courts are increasingly ruling on chargeback abuse cases, shaping legal precedents around merchant rights versus consumer protection such as vacating the FTC's "click to cancel" rule, limiting arbitration enforcement and how merchants handle chargeback mitigation.

- **Buy now, pay later fraud:** As BNPL adoption grows, merchants face legal risk when fraud occurs due to inadequate customer verification, poor refund handling, or deceptive marketing. Regulators in the US, UK and Australia are updating consumer lending rules that may increase merchant accountability for fraud-related losses and customer harm including handling disputes, refunds and fraud claims.

- **Money-laundering**: Merchants offering financial products face regulatory risk if they fail to implement adequate AML/KYC controls, potentially leading to fines, enforcement actions, and reputational damage due to their role in facilitating financial transactions.

- **Scams**: Merchants face consumer compliance risk from regulators like the FTC if their products or services enable scams (e.g., gift card scams), deceive or unfairly treat consumers, or lack appropriate refund, billing, or data practices — potentially resulting in fines, litigation and reputational damage.

Legal and compliance teams are playing a more strategic role in fraud mitigation.

Beyond guardrails: adding strategic value

Legal and compliance teams are playing a more strategic role in fraud mitigation — not just managing downside risk but enabling their companies to grow with confidence. Your involvement can help strike the right balance between protecting your business and preserving customer experience.

Finding that balance can be vital. Responding too slowly or not at all can expose your business to litigation, enforcement and brand erosion that undermines customer trust. But overcorrecting can be just as costly. Excessive fraud controls can slow onboarding, reduce conversion rates and alienate customers.

When you reframe fraud risk management as a cross-functional strategy tied to business outcomes, you're not just helping reduce exposure, you're helping shape how the business competes and earns trust by enabling faster onboarding, reducing false positives, aligning with evolving laws and improving operational efficiency.

> "Creating a governance structure that enables the business to consult with stakeholders early and often to enable swift, risk-based decision-making — while also providing clear guardrails for the business to operate — is critical."

Amy Schuh
Partner, Morgan, Lewis & Bockius LLP

Strategies for managing e-commerce fraud

Fraud happens. But with the right legal strategy, your team can manage the risk effectively while maintaining the overall customer experience. Start by taking these actions.

Build proactive defenses

Define clear terms of service

Strengthen your legal position by having your terms of service and fraud policies clearly outline how fraud is monitored and addressed.

Align fraud policies with legal exposure

Specify how customers can dispute fraud and how liability is allocated between merchants, payment processors and customers.

Audit fraud tools for effectiveness, bias and compliance

Work with fraud and product teams to evaluate whether systems are properly identifying fraud without disproportionately flagging certain customers. Create alignment with applicable anti-discrimination and privacy laws such as CCPA and GDPR. Document fairness audits.

Bolster fraud prevention measures

Position real-time fraud detection, multi-factor authentication for customer accounts and hardened customer identity verification as both a compliance necessity and a risk management priority

Establish fraud tolerance thresholds

Set fraud-level tolerance based on your business model, cost-benefit analysis and industry benchmarks. Develop monitoring protocols and incident response playbooks for when those thresholds are exceeded.

Create internal escalation protocols

Define when your team should be brought in based on fraud thresholds, regulatory risk or potential customer harm. Create specific internal procedures that include roles, timelines and documentation requirements.

Innovate front-line fraud controls

As e-commerce capabilities are designed, implement preventive and detective fraud controls upfront to help mitigate the risk of future issues.

Respond decisively when fraud hits

Develop your fraud incident response strategy

Anticipate the more likely fraud-related legal claims — ATO, chargebacks, false declines — and plan your legal defense in advance.

Maintain consistent documentation

Track fraud investigations, customer interactions and mitigation decisions in a way that supports legal defensibility and regulatory readiness.

Define regulatory response protocols

Establish when and how your team should engage with regulators and card networks. Keep response templates and roles clearly documented.

Establish law enforcement coordination protocols

Define when and how to engage law enforcement if there's a significant fraud incident. This can foster timely, effective cooperation and help preserve critical evidence for potential investigations or prosecutions of suspected bad actors.

Engage outside counsel proactively

Build relationships with fraud and enforcement specialists before you need them. Identify professionals with experience in fraud litigation and regulatory enforcement who can support you when incidents escalate.

Contacts

Ryan Murphy
Partner, Global Investigations & Forensics Leader, PwC US
ryan.d.murphy@pwc.com
LinkedIn

Devesh Desai
Principal, Financial Crimes Practice Leader, PwC US
devesh.desai@pwc.com
LinkedIn

Katrina Carrizales
Partner, Investigations & Forensics, PwC US
katrina.l.carrizales@pwc.com
LinkedIn

Brian Castelli
Principal, Fraud Management Leader, PwC US
brian.castelli@pwc.com
LinkedIn

Ted Trautmann, Lisa Meepummarin, Tucker Greer
Contributing authors