Ecommerce Solution Brief: Deliver Safe and Convenient Cross-Channel Experiences, Safeguarding Consumers from Fraud

**Business Benefits**

- **Protect revenue** by tackling chargebacks and losses due to fraudulent transactions.
- **Minimize operational downtime** due to fraud and continue providing reliable services.
- **Build long-term consumer relationships** by delivering consistent, secure and convenient experiences over every channel and interaction.
- **Ensure your business is compliant** with regulations for payment services, protecting consumers’ data and safeguarding from breaches.
- **Streamline the experience** and reduce friction for trusted consumers by assessing digital, physical and behavioral criteria and implementing risk-appropriate authentication techniques.
- **Improve transaction conversion rates** and accept more orders from trusted consumers by verifying and approving trustworthy transactions more accurately.
- **Harness the power of global shared intelligence** through LexisNexis® Digital Identity Network® and access data from billions of annual transactions across diverse industries, helping you make more informed risk decisions.

**Fraud Patterns Targeting the Ecommerce Industry**

Fraud can have serious consequences for ecommerce businesses that go beyond financial losses, including loss of consumers, legal issues due to compliance violations and reputational damage. Common types of fraud attacks targeting the ecommerce sector include:

- **Chargeback Prevention**
  Fraudsters may use stolen credit cards to make purchases and then later file chargebacks, leaving the merchant to face both the loss of goods and chargeback fees.

- **Account Takeover**
  Consumers often reuse passwords and login credentials across multiple platforms, making it easier for fraudsters to gain unauthorized access to their accounts. This puts both merchants and consumers at risk.

- **Refund Abuse**
  Consumers may abuse refund policies by repeatedly purchasing products, using them temporarily, and then returning them to receive full refunds. This practice can impact a merchant’s profitability.

- **Friendly Fraud**
  Consumers falsely claiming unauthorized transactions or filing chargebacks instead of resolving disputes directly with the merchant can lead to loss of revenue and increased chargeback fees. Merchants often struggle to differentiate between genuine cases and fraudulent chargebacks.

- **Promotion and Loyalty Fraud**
  Fraudsters have gained the ability to utilize stolen promotion/loyalty identities to acquire free products. This results in increased financial exposure for the merchant.
Fraud Patterns Targeting the Ecommerce Industry (continued)

**Shipping Fraud**
High value brand items like jewelry, clothing, video gaming consoles or luxury accessories are being maliciously acquired and shipped to locations inconsistent with prior purchase patterns and behaviors.

**Bot Attacks**
Automated bot attacks set up by fraudsters can disrupt an ecommerce site, steal data, make fraudulent purchases or perform other malicious actions. This type of attack is one of the most significant challenges for the ecommerce sector as it targets not just the conventional consumer touchpoints of new account creation and logins but also change of details events, which had the highest growth in bot attacks at 441% globally YOY in 2022 vs. 2021.1

**Card Testing**
Fraudsters attempt to verify stolen or cloned card details by making small transactions or “card testing” before initiating larger fraudulent purchases. This poses a challenge for merchants as they must identify and prevent such fraudulent activities.

Bot attacks targeting the ecommerce industry have risen significantly, with rates increasing by 195% globally in 2022 vs 2021.1

Prioritize Convenience and Safety Across Ecommerce Channels by Making Smarter Risk Decisions with LexisNexis® Risk Solutions
Consumers anticipate universally consistent, reliably secure and smooth experiences over every channel through interaction with an ecommerce business. The ability to combine convenience and responsive security across the consumer journey is becoming a competitive differentiator in crowded digital marketplaces. Ecommerce businesses failing to achieve that fragile balance face the detrimental impacts of costly fraud losses and significant consumer attrition.
Multi-layered Approach to Strengthen Fraud Prevention

Our multi-layered approach leverages market-leading identity verification, authentication, fraud detection, investigation and digital identity intelligence capabilities, helping you strengthen your fraud prevention strategy.

Authentication  Behavioral Intelligence  Digital Identity Intelligence  Document Authentication  Phone Intelligence  Physical Verification

Our solutions help ecommerce businesses tie together a 360-degree view of consumers across digital, physical and behavioral dimensions. By leveraging intelligence from all available channels, as well as from different industries using Digital Identity Network®, a global repository of intelligence which harnesses data from billions of annual transactions across diverse industries, ecommerce businesses can become better prepared to tackle both complex fraud and seasonal fraudulent events that could put legitimate consumers at risk. In the long term, ecommerce businesses can enhance their fraud prevention strategy, offer consumers an improved experience, optimize conversion in a safe and compliant way and expand their business with greater confidence.

For more information on our award-winning solutions, visit: