Expanding and growing markets will also mean higher risk of fraud, which in turn will require more advanced fraud prevention solutions.

Responses attributed to Monica Acree, VP of Sales, APAC, Forter

1. Why is fraud prevention important to gain customers' trust?

According to 451 Research, 69% of businesses believe they are prioritizing fraud prevention over user experience. An over-emphasis on fraud prevention negatively impacts genuine customers and revenue. Digital commerce is built on trust. At every point along the eCommerce journey, businesses must make a critical decision: *Can I trust this customer?* Answering this simple question accurately and instantly is powerful—it can accelerate revenue growth and strengthen your connection to customers.

2. How can you minimize lost revenue from digital fraud?

Digital fraud negatively impacts businesses in many ways. Not only does it cost businesses a loss in revenue, it also takes away time and resources spent on reviewing false positives, resulting in a negative customer experience. A risk averse approach to fraud prevention can cost businesses the potential of long-time customers, with businesses potentially losing up to 75x more revenue to false declines than they do to fraud. Research from Forter revealed that new shoppers are 5-7x more likely to have their purchase declined than returning users, in a phenomenon known as New User Missed Opportunity.

Retailers should instead look to advanced digital fraud prevention tools that enable them to move beyond traditional rules and manual reviews and stay one step ahead of fraudsters. This lets retailers reduce false declines without being bottlenecked by slow manual reviews and provides an opportunity to expand their service offerings. This not only increases revenue and approval rates but cultivates trust with their customers to build a long-term relationship.

3. What are the most common types of digital fraud?
The top three most common types of digital fraud are Account Takeover Fraud, Chargeback Fraud and Refund Fraud.

Account Takeover Fraud (ATOs) occurs when fraudsters gain access to legitimate accounts. These accounts may be compromised through stolen passwords, phishing schemes, or data breaches, allowing fraudsters to access the customer's stored payment instruments, personal data, loyalty points, and purchase history. ATOs can shatter the consumer's trust and affect brand reputation. Data from KPMG found that nearly one-fifth of respondents would no longer shop with a retailer if their personal information was hacked.

Chargeback Fraud is a form of policy abuse and is sometimes considered 'friendly fraud'. This is where the customer files false chargeback or refund claims despite having received their purchase. According to Forter, policy abuse is costing retailers in the United States over US$89 billion in annual revenue. Adopting fraud management technologies that can actively identify repeat abusers is key to scaling down chargeback fraud.

Refund Fraud is when a purchase is made using stolen payment information and refunded to an alternate credit card. Fraudsters can often trick the e-commerce merchant into issuing such a refund by claiming that the old credit card account is now closed and is a fairly simple, yet effective tactic that puts the retailer in a difficult position.

4. How can fraudulent transactions be minimized during large scale sales e.g. Black Friday on e-commerce platforms?

Many retailers rely on legacy fraud management models to combat fraud, such as manual review and rules-based decisioning. These are reactive in nature, and are hard to scale to match periods of large sales volumes such as Black Friday. Instead, advanced fraud prevention tools can tap into a network of data across enterprises, banks, payment providers and industries. This lets retailers build a better picture of a genuine customer, enabling both fewer customer declines and a smoother customer experience for new shoppers. These tools are also proactive and can adjust to new patterns of user behaviour, keeping up with a rapidly evolving consumer landscape. These tools also create the means to segment customers by risk, enabling frictionless digital experiences—and higher satisfaction levels—for lower risk customers.

5. How can retailers build an abuse resistant returns system?

The challenge in dealing with policy abuse such as returns fraud is that it is committed not only by fraudsters, but also by legitimate customers. Many businesses rely on traditional fraud solutions and internal review processes to tackle this challenge. However, these can be ineffective as they are meant to identify fraudsters, not customers abusing policies. The right first step is to understand the type and magnitude of abuse. The second step is identifying repeat abusers. And then a natural third step is to adjust policies in real-time based on the identity behind a transaction—specifically, a repeat abuser can purchase items as final sale (with returns not an option).

6. How does it feel to be a woman leader in technology? What would be your words of advice for the younger generation of emerging leaders?
As a woman in a male-dominated industry, representation at the top is essential. Some women may hold back feedback or opinions due to the fear of negative impact. As a leader who is direct and

open by nature, I continue to be authentic to myself to challenge these gender norms. I also make sure to create a safe space for my young female co-workers to do the same as well.

My advice to emerging leaders is to always adopt an open learning mindset, and constantly hone your skills. Setting aside time every day to learn and digest the wealth of content out there will give incremental gains that set the stage for great personal growth.

7. What do you predict are the trends for the next five years that will influence digital retail fraud prevention?

The rapid uptake of digital retail has been accelerated by the COVID-19 pandemic and has made e-commerce even more convenient and accessible. With the eCommerce market in India expected to grow by US$140 billion by 2026, the next five years are likely to see further penetration at all ends of the consumer markets both up and down, further growing the customer base. Expanding and growing markets will also mean higher risk of fraud, which in turn will require more advanced fraud prevention solutions.