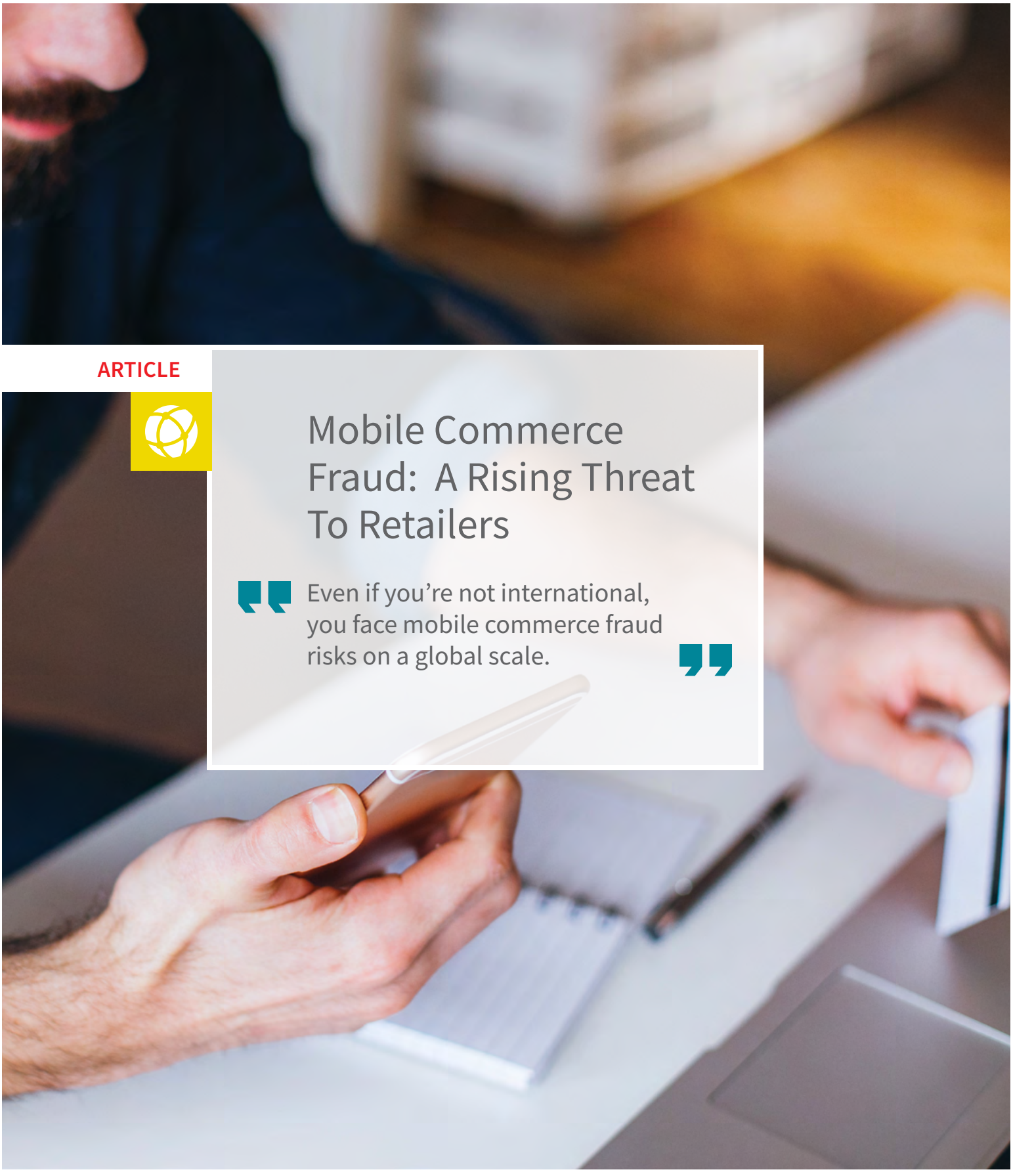
LexisNexis®
RISK SOLUTIONS



ARTICLE

Mobile Commerce Fraud: A Rising Threat To Retailers

> Even if you're not international, you face mobile commerce fraud risks on a global scale.

ARTICLE

Whether you're a growing regional business or a multinational brand, the move to mobile opens your doors to literally everyone, everywhere. With the rapid growth of international transactions come new risks and fraud considerations. Unique regulations and financial initiatives across the globe create special challenges for mobile retailers trying to quickly verify consumer identities, transaction origination and payment methods.

Retailers newer to the mobile channel say that fraud attempts have increased in the past year.

Mobile and global: A correlation

Our 2019 True Cost of Fraud™ Study of e-commerce merchants finds that retailer segments experiencing the most growth in mobile channel adoption also see the most growth in international transactions. Of note: Among small retailers with m-commerce that sell digital goods, 21% of transactions are now international versus domestic-based—an 8% increase from 2018. For mid/large retailers with m-commerce that sell physical goods only, international accounts for 29% of transactions—up 18% from 2018.

Some of the factors that contribute to m-commerce fraud:

Consumer Identity Verification: Regulations such as the General Data Protection Regulation (GDPR) limiting access to consumer data make it much more difficult to verify a consumer's identity. As consumer privacy continues to be a concern among regulators, fraud prevention strategies relative to consumer identity verification should be continuously reviewed. Merchants need to use tools that provide insight into digital identities that inform characteristics such as device/e-mail/URL/IP addresses and digital behaviors.

Alternative Payment Methods: As governments and industries globally explore alternative payment methods, such as Bitcoin, retailers will be tasked with the challenge of how to verify the method. For example, India demonetized some of their cash currency in 2018, encouraging the move to digital payments.

Transaction Origination: Retailers in our Study cited this as a top mobile channel challenge when selling digital goods. While IP addresses are often a useful tool in determining where a transaction originated, they are not always device-specific, provided by the network the device is on. Thus, traditional fraud detection solutions built around IP address assessment may prove less effective.

You can survive fraud attempts—and thrive despite them.

Go for new growth opportunities without adding risk to your business. Download the LexisNexis® Risk Solutions 2019 True Cost of Fraud™ Study: E-Commerce/Retail Edition for the latest insight.

For more information, call 800.869.0751 or visit risk.lexisnexis.com/risk/retail

LexisNexis® RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict, and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information and analytics for professional and business customers across industries.