

Data accessibility **versus** data security— a dangerous balancing act

Financial institutions in Asia realize that access to current, accurate customer data is key. But securing data and preventing fraud is a constant challenge that is impacting e-commerce growth.¹

Banks are fighting fraud with



Multi-factor authentication



Biometrics



Device assessment

Cutting-edge, multi-layered authentication technologies are becoming a reality



Knowledge Based Identity Authentication – quizzes are frequently utilized, but more advanced technology including geolocation, customer profile data analysis and device identity fingerprinting are used by fewer than 40% of financial institutions²



Machine Learning and Robotic Process Automation (RPA) – can conduct innocuous tasks better suited to technology for increased efficiency



Artificial Intelligence – combined with behavioral biometrics can detect customer inconsistencies



Distributed Ledger Technology (DLT) – combats fraud by enabling the storage and transmission of secure, immutable data

Are you embracing these emerging technologies?

The cost of failure in meeting data privacy requirements are steep...



- EU – EUR 20 million
- Singapore – SGD 1 million
- Australia – AUD 1.7 million

And regulators are increasingly sharing intelligence to detect, prevent and disrupt crime



- Hong Kong's Fraud and Money Laundering Intelligence Taskforce (FMLIT)
- Singapore's AML/CFT Industry Partnership (ACIP)
- Australia's Fintel Alliance

To learn more about cutting-edge customer data security and accessibility
visit risk.lexisnexis.com/ID-EN



¹ <https://www.emeraldinsight.com/doi/abs/10.1108/ICS-05-2015-0020>

² LexisNexis® True Cost of Fraud™ Study

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. True Cost of Fraud is a trademark of LexisNexis Risk Solutions Inc. Other products and services may be trademarks or registered trademarks of their respective owners. Copyright © 2018 LexisNexis. All rights reserved.