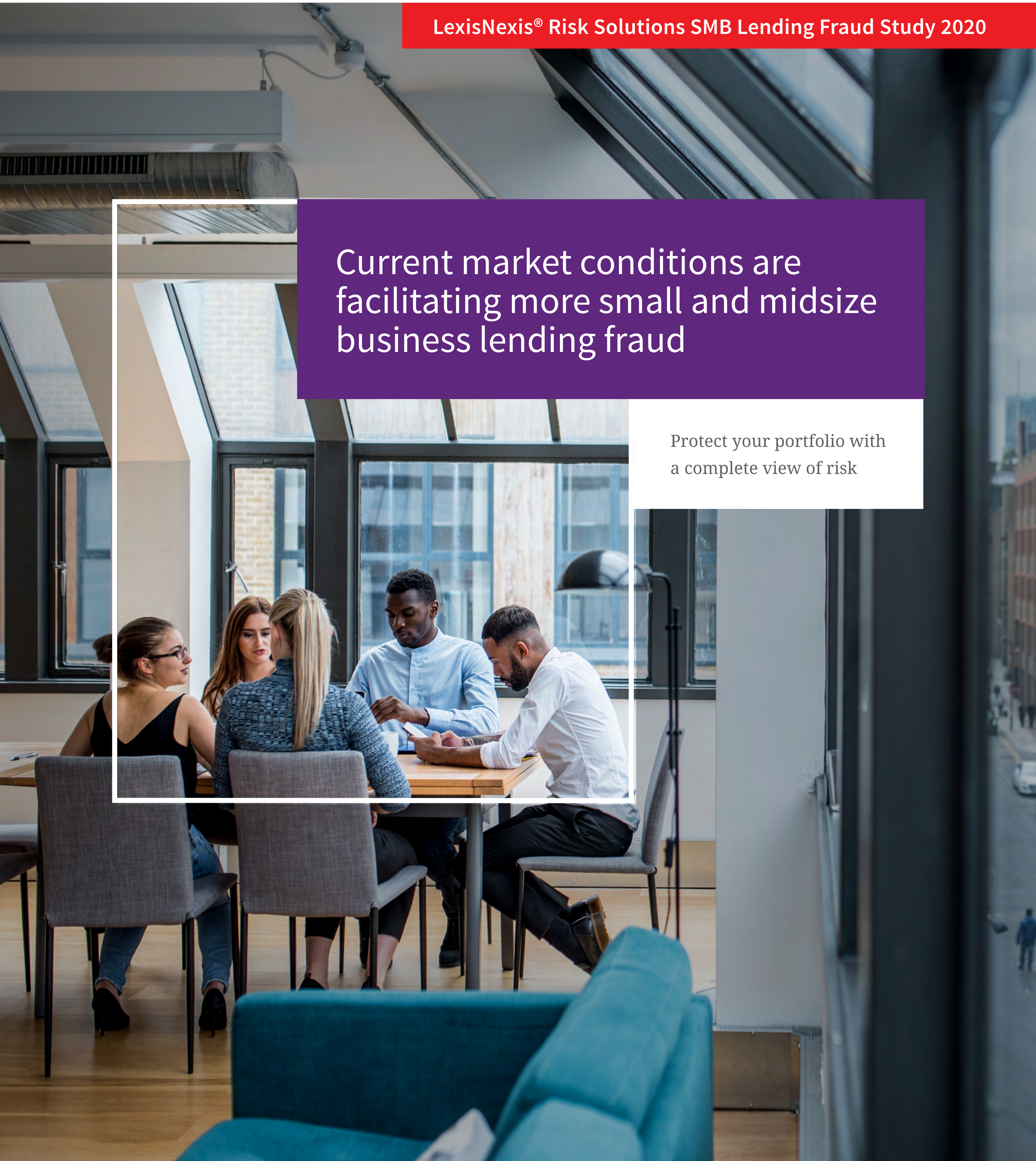
LexisNexis® Risk Solutions SMB Lending Fraud Study 2020



Current market conditions are facilitating more small and midsize business lending fraud

Protect your portfolio with a complete view of risk

A multi-layered SMB fraud prevention strategy helps your business focus on viable lending opportunities and foster stronger portfolio performance

Fraudsters are capitalizing on rapidly changing market dynamics

Fraud follows opportunity and as controls and prevention efforts around consumer fraud become more sophisticated, fraudsters are turning their attention to small and midsized business lending fraud (SMB fraud). With more lenders offering omni-channel transaction experiences, the chances to commit fraud are multiplying and fraudsters are fully capitalizing on the opportunities. Our recent study illustrates the high stakes of fraud with input from 135 SMB lenders representing a mix of small and midsized banks, fintech and digital lenders, credit unions and payment processors.

- SMB lending fraud is steadily rising, with the average lender experiencing an 8.3% increase in fraud over the last 24 months.[1]
- Fraud losses as a percentage of revenue have increased an average of 28.6% year-over-year.[2]
- A successful SMB fraud attempt delivers high-value returns – the average small business loan amount in 2017 was $107,000.[3]

As these factors coalesce within today's rapidly changing business environment, your business could be exposed to the damaging impacts of SMB lending fraud:

- Loss of revenues
- Declines in portfolio performance
- Reputational damage
- Exposure to liabilities
- Costs associated with missed opportunities

The current level of fluidity across global markets and acute contractions in the small business sector only exacerbate the challenges of SMB fraud and provide more routes for it to flourish. The decisioning speeds and high levels of pressure to quickly distribute loans under recent stimulus packages are expected to contribute to loan fraud rates of 10-12%.[4] SMB loan applicants are also interfacing with your business over digital and online channels more than ever before. Protecting your business against SMB fraud is paramount to maximizing portfolio performance and revenues and the best defense demands a complete view of risk.

Defining the fraud risks that are specific to small and midsized businesses

Small and midsized businesses represent unique and nuanced fraud risks. Well-informed decisions require visibility into the business itself as well as a deep understanding of the authorized representatives tied to the business. The connections between people and businesses are elements that SMB fraudsters specifically exploit to commit fraud. The complex layers of identity and financial attributes associated with businesses and people combine to facilitate an ideal environment for several types of fraud, including:

- **Synthetic Identity Fraud:** Creation of a new identity/business entity using a combination of real and fabricated information, or sometimes entirely fictitious information, to commit fraud
- **Third-Party Identity Fraud:** Identity theft of true owner/authorized business representative to commit fraud
- **Third-Party Account Takeover Fraud:** The use of a combination of a victim's Personally Identifiable Information (PII) to access an associated financial account in an effort to fraudulently secure a loan
- **First-Party Friendly Fraud:** Business owner/authorized user or individual associated with business owner (i.e. family member, friend, etc.) commits loan fraud
- **Loan Stacking:** Utilizing several different taxpayer identification numbers to obtain multiple loans for the same small to midsized business
- **TIN-Spoofing:** Creation of multiple taxpayer ID numbers to fraudulently apply for loans

To further complicate the SMB fraud scenario, sophisticated individual fraudsters and well-networked fraud rings are adept at test-driving the fraud defenses and controls among several lenders. Once system vulnerabilities are uncovered, fraudsters quickly target and exploit these weaknesses by funneling as many loan applications as possible through those lenders. Fraudsters continually adapt and shift their schemes to capitalize and monetize the most viable route to quick and often, undetected, profits, meaning your fraud defense strategy needs to be highly dynamic and risk-responsive.

Identify and proactively prevent SMB fraud

The right tools and layered technology support a proactive fraud strategy that creates an advantage in identifying and preventing SMB fraud. LexisNexis® Risk Solutions can develop a multi-layered fraud defense that easily adapts to help you respond to today's changing SMB risk climate.

We combine our extensive coverage of small to midsized businesses and their associates with proven analytics to provide a clear, unified illustration of the critical relationships and connections within a business. By layering this comprehensive view of a business with our advanced fraud detection solutions, we can help automate lending decisions and isolate fraud before it enters your portfolio. Our fraud solutions integrate physical and digital identity intelligence with device, biometric and behavioral insights to enable your business to quickly detect fraud signals and stop enterprising fraudsters in their tracks. With an optimal fraud prevention strategy, you can focus on viable lending opportunities and foster stronger portfolio performance. Protect against SMB fraud and prioritize core business objectives with LexisNexis Risk Solutions.

CASE STUDY

The following scenario illustrates how our analytics team works to help our customers identify and prevent SMB fraud.

Opportunity: A company wanted to develop a fraud model for new SMB customers.

The Model:

- We created a segmented model to address the problem (business only, business owner/authorized representative only and blended business and business owner/authorized representative).
- There were three types of fraud: first party fraud, identity fraud (assumed to be stolen or manipulated identity) and other.
- Many top attributes in the model were related to phone verification and distance fields such as distance from the business address to representative address.
- An outcome of the analysis showed some counterintuitive relationships where businesses with high sales, but great distances between input address elements or other identifying input elements on file were high risk. This may suggest that business entities were being stolen by fraudsters.

Results in the lowest scoring 5% of the populations:

23% of the business owner / authorized rep frauds were identified
24% of the business only frauds were identified
40% of the blended (business and business owner information) were identified

Implementation: The customer deployed the blended score immediately and is also using LexisNexis® InstantID® Business for identity verification.

For more information:
Call 800.897.1644 or visit risk.lexisnexis.com/SMBRisk

1. and 2. LexisNexis® Risk Solutions US SMB Lending Fraud Study, April 2020
3. Shepard, Maddie, "Average Small Business Loan Amounts, Broken Down and Explained," Fundera, https://www.fundera.com/business-loans/guides/average-small-business-loan-amount, April 4, 2020
4. Prior, Jon, "Bankers fear massive fraud in PPP", American Banker, americanbanker.com, May 7, 2020

LexisNexis®
RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis.