WALKING THE TIGHTROPE BETWEEN FRAUD & FRICTION

How digital & physical identity can curb both omnichannel risk and friction

An abstract from the LexisNexis® Risk Solutions 2018
State of Risk in Communications, Mobile & Media

LexisNexis®
RISK SOLUTIONS

YOU KNOW WHAT YOU'RE UP AGAINST WHEN PURSUING MARKET SHARE.
**WITH A BALANCED STRATEGY, YOU'LL PREVAIL.**

Success in today's highly competitive Communications, Mobile & Media landscape depends on an elevated customer experience and an ability to seize opportunity, while mitigating a diversity of threats throughout the customer journey.

In this four-part series, LexisNexis® Risk Solutions examines some of the most common risks facing Communications, Mobile & Media as they navigate massive industry transformation, the role of identity data and best practices for managing the tension between mitigating risk and creating an elegant customer experience.
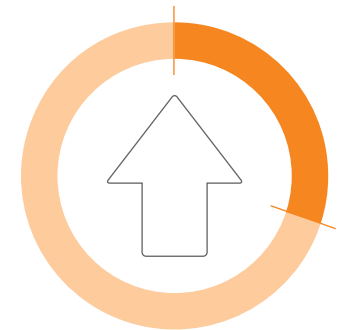
Risk Spotlight: An Omnichannel Approach

Increasingly, customers engage through multiple touch points—even for a single transaction. This eBook explores the challenges and best practices for cross-channel customer journeys. Getting it right is critical, as you can see from the stats below.

What's an omnichannel customer worth?[1]

15% **35%**

15-35% increase in average transaction size

5% **10%**

5-10% increase in loyal customer experience
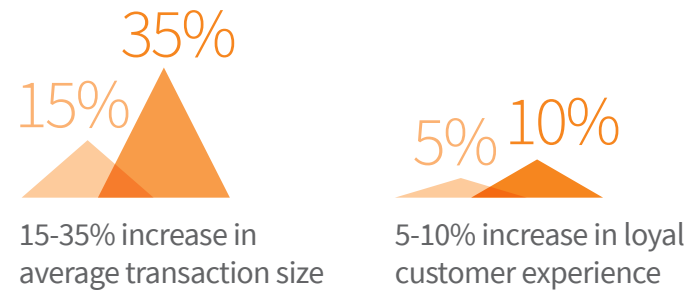
30% higher lifetime value
over those that use only 1 channel

LexisNexis®
RISK SOLUTIONS

FRICTION DOESN'T HAVE TO BE A DIRTY WORD.

Before we dive into the use of identity data to mitigate fraud while improving the customer experience, it's important to understand a few things about friction:

First, the truth about friction:

A "frictionless" customer journey doesn't equate to an absolutely friction-free experience. It's about having the right type of friction, with the right action, at the right time. You have to figure out where and what that is.

Friction helps to provide trust and confidence—but the priority is to confirm an activity is legitimate.

The problem is that friction—and the customer frustration it causes—is inherent to traditional methods of mitigating risk.

Step-up authentication without proper context just results in repeat interruptions—not risk mitigation.

Malware, SIM swap, re-direction and social engineering fraud are designed to circumvent step-up authentication anyway.

The opportunity:

Use digital and physical identity tools in new ways that mitigate risk and also enhance the customer experience.

Example: When you combine digital identity and traditional identity-based risk services at new account opening, you start to accumulate trust data from the start. It becomes easier to replicate frictionless experiences and mitigate risk through the rest of the customer journey.

Walking the Tightrope Between Fraud & Friction: An abstract from the LexisNexis® Risk Solutions 2018 State of Risk Report

3

LexisNexis®
RISK SOLUTIONS

DIGITAL IDENTITY: IT'S NOT JUST FOR DIGITAL EXPERIENCES ANYMORE.

The growing volume of digital identity data being collected may be leveraged outside of digital interactions —for example, at the retail counter or call center.

Digital identity should be your "First Layer Defense" because it solves for the most complex use case (mobile device interactions).

Key pieces of those frictionless digital-first workflows can also facilitate more consistent, seamless person-to-person experiences across all other channels.
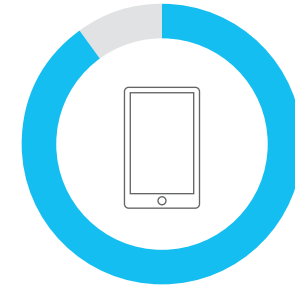
It's a sound strategy even if the majority of your sales and customer interactions occur in the store or call center.
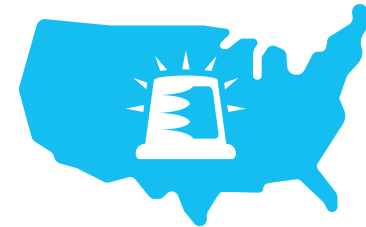
The dynamics of digital identity adoption:

Ubiquity of mobile

>90% of all transactions involve mobile at some point in the customer journey[2]

829 U.S. data breaches exposed over 2B individual records in 2017[3]

Reliability and security of digital identity data vs. traditional PII and physical ID

With digital identity data, a person's digital history is anonymized. Sensitive data is replaced with non-sensitive equivalents that can't be converted to PII.

Development of robust digital identity solution networks

It takes a network to fight a network. Fraud is a team sport, so you have to play team ball to fight it.

LexisNexis®
RISK SOLUTIONS

LAYERED DIGITAL IDENTITY + RISK SOLUTIONS = CUSTOMER JOURNEYS CALIBRATED TO RISK

Every company's workflow is unique, but best practice calls for consistent application of digital identity paired with thoughtful risk-based use of other risk solutions such as decision analytics, verification and authentication, and where necessary, investigation and review products.

This coordinated, comprehensive approach sets the stage for reduced friction and an enhanced customer experience. Here are a few helpful recommendations to get you started:

Start with identifying all of your key digital customer experience interactions (i.e. account opening, logins, payments, account information changes, etc.).

Implement a digital identity solution network throughout all of them—one robust enough to mitigate account takeover risk, reduce customer friction and gather ample "trust data" around customers and their linked devices. The goal is to tag the greatest percentage as "trusted."

Workflows should be personalized and differentiated at each experience point. Example: device fingerprinting and linking across devices.

Consider ways to apply pieces of digital workflows to create frictionless, consistent experiences in "human" channels (i.e., store and/or call center).

In addition, you might bind the digital identity to physical identity with consent. This eliminates repetitive authentications that burden your customer.

LexisNexis®
RISK SOLUTIONS

MULTIPLE LAYERS OF DEFENSE:
ONE SHARED INTELLIGENCE NETWORK.

First Layer of Defense: Digital & Identity Intelligence

Customer Identity Data	Web & Mobile Device Intelligence	True Geolocation, VPN, Proxies & TOR	Malware & Bot Threat Detection	Behavioral Biometrics

Second Layer of Defense: Decision Analytics

Industry Best Practices & Decision Policies	Identity Correlation & Linkages	Behavioral Analytics & Variation	Machine Learning	Integration & Orchestration

Third Layer of Defense: Verification & Authentication

Identity Resolution, Attributes & Anomalies	Device Binding, Secure Notification & OTP	Dynamic KBA	Biometrics	Document Authentication

Fourth Layer of Defense: Investigation & Review

Forensics & Investigations	Case Management & Workflow	Reporting	Feedback, Audit & Policy Governance

Walking the Tightrope Between Fraud & Friction: An abstract from the LexisNexis® Risk Solutions 2018 State of Risk Report

6

LexisNexis®
RISK SOLUTIONS
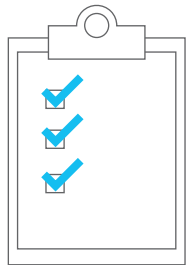
DON'T SETTLE FOR THE STATE OF RISK IN TODAY'S MARKET.

Fight back with the full power of LexisNexis® Risk Solutions.

Our capabilities include:
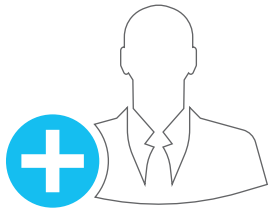
Identity Verification
- Validate name, address and phone info
- Reconcile variations, duplications and inconsistencies; link data points
- Perform global identity checks with seamless integration and reporting

Identity Authentication
- Authenticate identities on the spot using knowledge-based quizzes
- Dynamically adjust security level to suit risk scenario
- Receive real-time pass/fail results
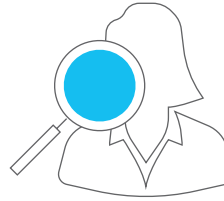
Premise Association Risk
- Assess the risk associated with opening an account
- Uncover potential "name game" fraud
- Determine if further investigation is needed
- Identify potential delinquent accounts for review
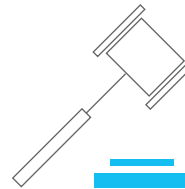
Credit Risk
- Access alternative data to understand a customer's holistic picture of risk
- Provide a risk score across all behaviors and media
- Prioritize fraud management action based on level of risk
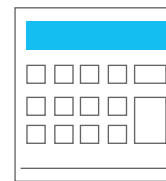
Fraud Scoring
- Quickly detect fraud patterns and isolate high-risk transactions
- Resolve false-positives and address verification system failures

LexisNexis®
RISK SOLUTIONS

Customer growth.
Lower risk.
Better customer experience.
What's not to like?

Contact us at
risk.lexisnexis.com/StateofRisk2018

LexisNexis®
RISK SOLUTIONS