

IS THE RIGHT RECIPE

Discover the right mix of digital identity
data to serve different business needs

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



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: The Many Faces of Digital Identity Data

It takes many forms and has multiple uses—but when **it's misused, it can also add friction and open doors to fraud.**

In this installment, we'll look at the use of digital identity data—how it's defined, and how Communications, Mobile & Media organizations are using it to manage against common risks like fraud and involuntary churn due to non-payment.



WHAT IS DIGITAL IDENTITY DATA ANYWAY?

Communications, Mobile & Media providers seem to have varying definitions of what constitutes digital identity data.

The official word from TechTarget is this: A digital identity is the body of information about an individual, organization or electronic device that exists online. It is derived from the use of information on the web and from an individual's actions online.¹

Examples of Digital Identity Data:



Email



Cookies/Browser
Fingerprint



Phone



Location-based
Device Info



IP Address



Device ID



Social Media
Behavior



Behavioral Data

What It Isn't:



Credit Reports



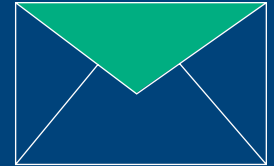
Scanned
Documents

On the following pages, we'll take a look at some of the most common types of digital identity data used across the industry—and the benefits and challenges of each.

¹ TechTarget, Definition: Digital Identity, 2018

EMAIL

As a form of digital identity, email tends to be a stronger tool for marketing applications than fraud prevention, although there is value to be gained in both areas.



BENEFITS:

Identity Verification

- Speeds onboarding to minimize friction
- Reduces fraud associated with hacked emails, which are used to obtain additional services using fraudulent credit cards

Marketing

- Improves targeting efforts
- Reduces marketing costs

DRAWBACKS/CHALLENGES:

Identity Verification

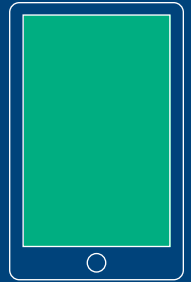
- Provides limited information on its own; must combine with other sources to glean full background and risk
- Data can be stolen/compromised
- Must rely on input from customers, who may resist
- Difficult to authenticate outside of remote channels
- Doesn't support behavior tracking, assessment
- Consumers use multiple emails

Marketing

- Consumers use multiple emails
- Isn't necessarily linked to one individual; can have multiple users within a household

PHONE

Providers often use caller ID and phone numbers for identity verification at onboarding. However, numbers can easily be spoofed, and additional network data that might be used for detection is often regulated.



BENEFITS:

Identity Verification

- ANI (Automatic Number Identification) significantly reduces call center fraud risk by identifying calls originating outside the U.S. or one's operating territory
- Also reduces customer friction and false positives

DRAWBACKS/CHALLENGES:

Identity Verification

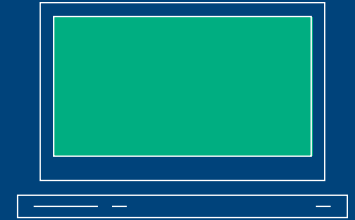
- Doesn't necessarily provide fraud/risk profile for an individual; can only confidently be linked to data at a household level
- Concerns that use of network behavior data for fraud assessment is non-compliant

Marketing

- Data is regulated for use in marketing and sales (CPNI)

IP ADDRESSES

IP addresses can help identify point of origin and distinguish fraud with significant savings. But the advent of new technologies has significantly reduced their reliability.



BENEFITS:

Identity Verification

- Improves identification of botnet attacks
- Enables faster onboarding to reduce friction
- Reduces account takeover victimization and fraud
- Helps to (generally) identify country and geographic location

Personalize Customer Experience

- Improves ability to customize offers

DRAWBACKS/CHALLENGES:

Identity Verification

- IP addresses are often dynamic and difficult to track
- Multiple users can have the same IP address



Within a household

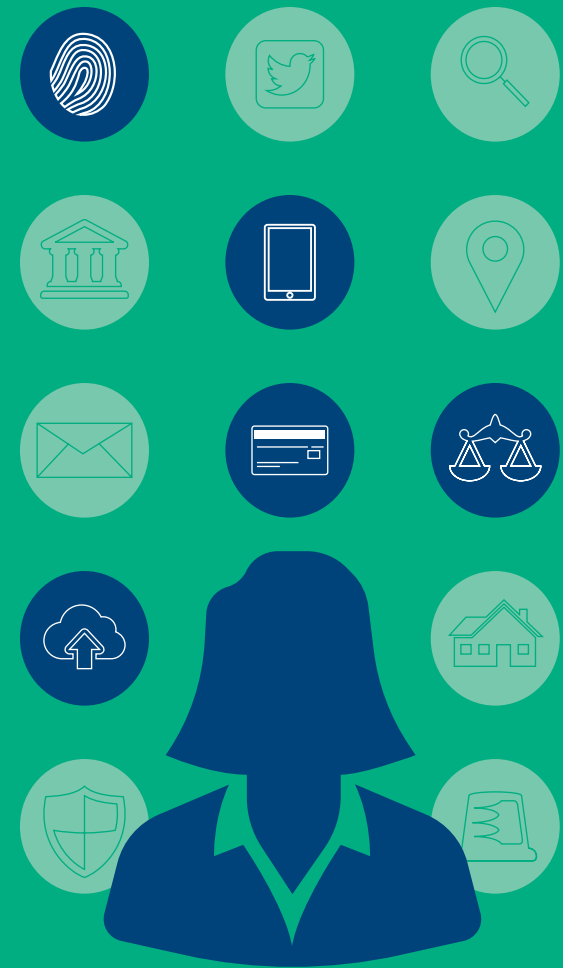


When the ISP is using network address translation (NAT) to route users

- Fraudsters can obscure IP addresses through proxies, VPNs or connections to botnets
- Assessing if an IP address is masked can require heavy manual effort

As you consider available types of personally identifiable information and anonymous digital identity data available, keep in mind no single type can do it all.

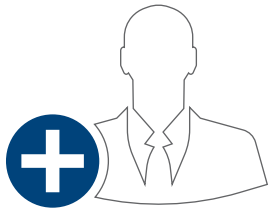
Test varying types in your fraud scoring and measure against your objectives to determine what combination works best at each point of vulnerability in your customer journey.



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

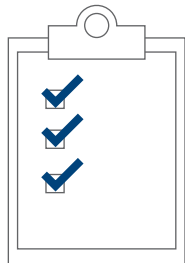
Fight back with the full power of LexisNexis® Risk Solutions.

Our capabilities include:



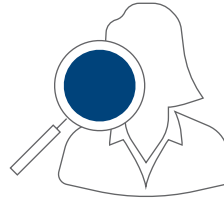
Identity Verification

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



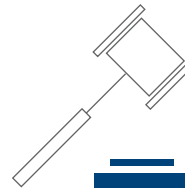
Identity Authentication

- Authenticate identities on the spot using knowledge-based quizzes
- Dynamically adjust security level to suit risk scenario
- Receive real-time pass/fail results



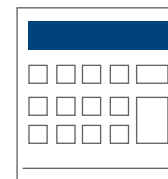
Premise Association Risk

- 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

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

Contact us at
risk.lexisnexis.com/StateofRisk



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.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. LexisNexis Fraud Multiplier is a service mark of RELX Inc. Copyright © 2018. NXR12574-00-1018-EN-U