

# FALSE PROMISE

That high-value prospect could  
be a synthetic identity

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: Synthetic Identity Fraud**

The ever-increasing number of identity data breaches has made it easier than ever for cyber criminals to obtain the critical seeds for synthetic identities. Because it often appears as “Never Pay/Bad Pay,” and often has no real victim, synthetic identity fraud has become one of the most insidious forms of identity fraud plaguing organizations today.

“It’s difficult to determine actual fraud losses associated with this type of fraud because credit issuers very often do not properly classify losses as fraud; rather, they are sent to the collections department for resolution.”<sup>1</sup>

- **Philip Bartlett**, inspector in charge, New York Division,  
U.S. Postal Inspection

**False Promise:** An abstract from the LexisNexis® Risk Solutions 2018 State of Risk Report

<sup>1</sup> As quoted in Fraud Magazine, “To Snare A Menace”, Nov/Dec 2016

## WHAT IS SYNTHETIC IDENTITY FRAUD?

Synthetic identities are comprised of real and/or fake personal information. They are created by using information from either:



### **Multiple persons to create a single fake identity**

Valid shipping address from Person 1 + SSN and name from Person 2 + DOB from Person 3

This type may be used for shorter-term gains, such as purchasing big ticket items before getting caught



### **One person, using some of a person's information combined with fake data**

A real SSN + a fake name

Likely to be nurturing this identity, establishing a good credit history before ultimately “going bad” by fraudulently purchasing higher ticket items.



### **No known persons**

Fully fake data (DOB, Name, SSN)

This form also takes a longer, nurturing view toward fraudulent use.

## WHY IS SYNTHETIC IDENTITY FRAUD AN ISSUE FOR COMMUNICATIONS, MOBILE & MEDIA?

Synthetic identities are typically used by fraudsters in longer-term schemes. They seek out services that can help establish a footprint and nurture good credit.

Because full identities aren't composed from a single person, there likely won't be a victim to report the misuse—at least in the short term. This makes synthetic identity fraud particularly insidious. Profiles appear to be legitimate and high-value.

**Communications, Mobile & Media companies are a rich target for many reasons:**



The nature of monthly service makes it possible to nurture an identity profile and establish trust over time.



They serve a diverse clientele—including consumers with limited-to-no existing credit footprint to use in vetting.



Besides the services, fraudsters also have access to devices and equipment that can be sold for profit or used to seed additional synthetic identities.

## COMBATING SYNTHETIC IDENTITY FRAUD IS A TEAM SPORT.

While the fraud department will have the most knowledge of synthetic identity fraud, it's an enterprise and industry responsibility.

Those involved in account onboarding and management need to know the signs—and fight it from the front lines. And organizations must team up and collaborate to best shut it down.

Piecemeal solutions applied in isolation aren't effective enough. They leave gaps in visibility that skirt detection. You need a combination of insights.



Breadth and depth of identity data sources



Advanced linking and intelligent algorithms to help you spot patterns



Deep expertise in the online retail domain



A platform that can help you adapt as fraud schemes evolve

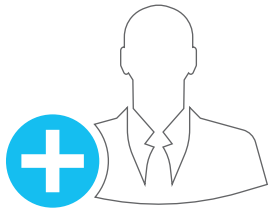
To take it a step further, it's critical to determine not only that the identity is real and that identity elements resolve to a single profile (identity verification), but also that the identity belongs to the person presenting it (identity authentication).

It's critical to work together by sharing information across the organization and the industry. Insights should be made available in real time—especially in fast-moving organizations that onboard customers and dispense equipment quickly.

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

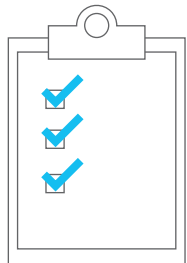
## Fight back with the full power of LexisNexis® Risk Solutions.

**Our capabilities include:**



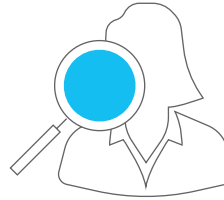
### **Identity Verification**

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



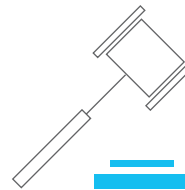
### **Identity Authentication**

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



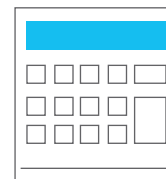
### **Premise Association Risk**

- 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](https://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. NXR12575-00-1018-EN-US