LexisNexis®
RISK SOLUTIONS

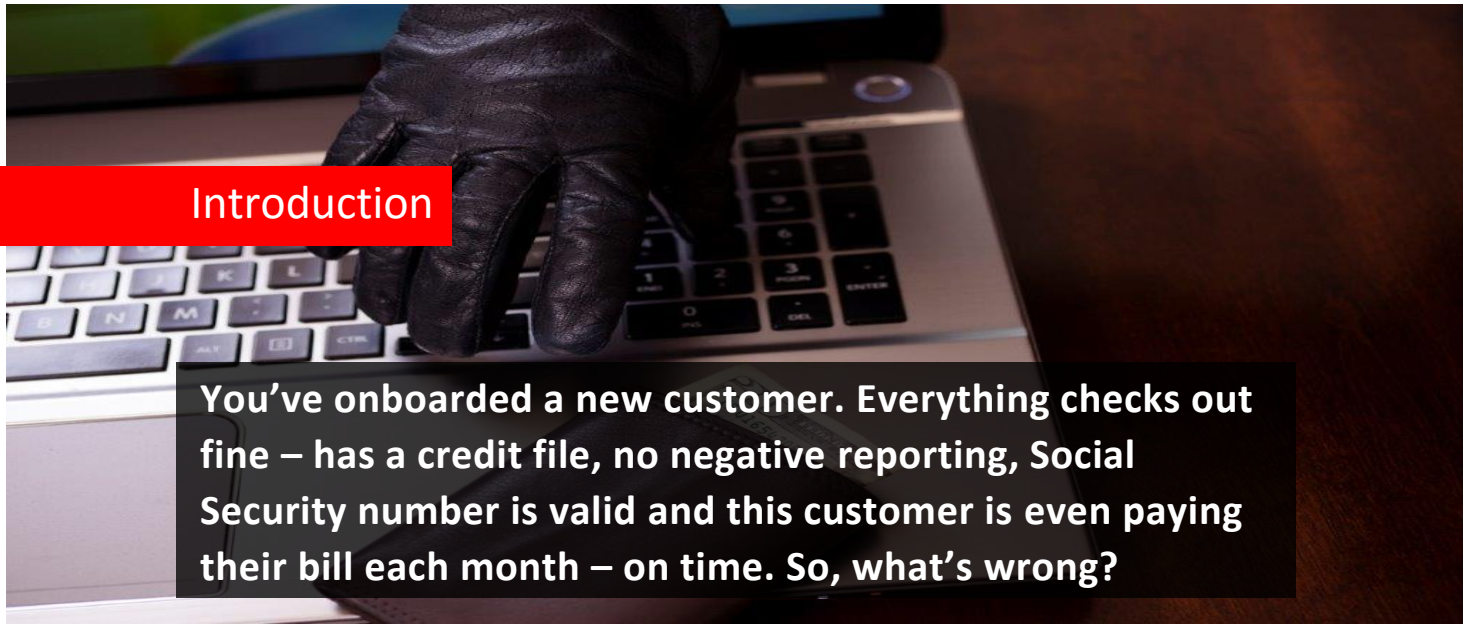
WHITE PAPER

State of Risk Series, Vol. 3

Communications & Media Services Companies are Key Targets for Identity Fraud.

These Fraudsters are Smart. Fighting Them Requires Smartly Layered Solutions Technology.

September 2017



Introduction

You've onboarded a new customer. Everything checks out fine – has a credit file, no negative reporting, Social Security number is valid and this customer is even paying their bill each month – on time. So, what's wrong?

It turns out that this customer is a real person, but is using a fake identity.

This is an ongoing concern for Communications and Media Services companies. The rise of synthetic identities has made it much more difficult to distinguish between legitimate and fraudulent customers. The use of fake identities is generally not for innocuous means; it's often to support a larger criminal enterprise. The challenge of detecting it can translate into more false positives and customer friction, making it more difficult for providers to balance fraud protection with the customer experience in a hyper competitive market.

"Any time you ask, "I need you to bring more information. I need you to show me proof of something. I need you to answer some questions" – you're going to lose some of the applicants, including some of the good ones. So, you try to minimize that." *(Credit Fraud Strategy Director, Nationwide Wireless Provider)*

We have conducted a comprehensive study that analyzes the State of Risk in the Communications and Media Services market. Through in-depth interviews with executives responsible for consumer marketing, fraud and account management, we've identified key issues around credit risk, fraud and identity management throughout the customer lifecycle affecting prospecting, onboarding and customer friction / churn / retention. These issues are highlighted in four State of Risk reports, each discussing a different set of lifecycle risks and ways Communications and Media Services companies can mitigate them.

Welcome to the third of four reports, focusing on identity fraud.

Our findings represent Communications and Media Services organizations across a broad range of products and services, from those offering wireless voice and data, mobile Internet, satellite TV and streaming media to traditional voice, cable, broadband and Internet service.

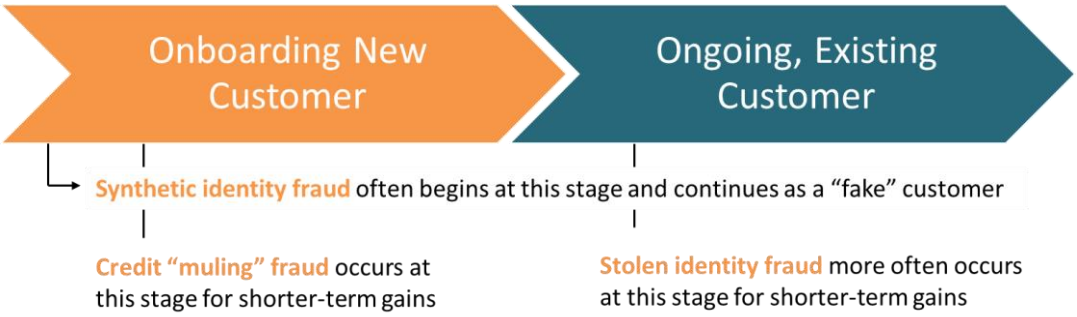
The Threat of Identity Fraud

Identity fraud is a concern for Communications and Media Services organizations, occurring at different stages of the customer lifecycle.

Identity fraud typically occurs through one of two ways: 1) stealing a real person's identity in order to obtain goods and services (stolen); or, 2) creating a fictitious identity in order to do the same, based on a combination of real and fake personal information (synthetic).

There's also another type of fraud that targets Communications and Media Services organizations that sell devices in retail stores; this is often called credit "muling". While not identity fraud per se, because it involves a real person using their own identity, the transaction is nonetheless being made on behalf of a criminal network. The purpose is to entice a person to enter a provider's retail store, use his / her own credit and identity to establish a service plan, obtain multiple devices without activating them and then hand those devices over to the criminal network afterwards in exchange for a cash payment. The criminals then re-sell the devices for a profit and payment is never made on the service plan - the provider has lost both the devices and the assumed revenue stream.

Credit "muling" fraud occurs at the front-end of the customer lifecycle stage; synthetic identity fraud begins at this point as well and continues as a fake account for a period of time; and stolen identity fraud typically occurs with existing accounts.



"So, credit muling is an issue right now. They're taking advantage of service providers' desires to gain new customers, and they're using their own information and credit to obtain the maximum number of devices and lines of service as they can with zero intent to pay." *(Director of Fraud Investigation, National Wireless Provider)*

The Threat of Identity Fraud

When stolen identity fraud occurs with established accounts, it is typically to obtain devices / equipment and services that can be used until detected by the victim.

Professional fraudsters are able to exploit data breaches across various sectors, along with consumer laxity around the strength and re-use of the same password across accounts; this helps them gain entry to various types of accounts, including those of Communications and Media Services customers. From there, fraudsters can order additional devices, or add / use the customer's services until being caught; examples include hijacking calling plans for use by scammers and adding video / gaming to newly ordered devices. Since this involves a real customer who will ultimately notice and report fraudulent activity, it typically focuses on the short-term gain.

"With all these breaches, there's organized crime harvesting names and passwords associated with various accounts and then they're going online, posing as the customer, and getting those devices shipped. We experience a lot of losses associated with add-a-phone." *(Director of Fraud Strategy, National Wireless Provider)*

The focus with synthetic identity fraud is more often long-term.

The key objective of synthetic identity fraud is to develop and nurture a credit history that makes detection more difficult by behaving as much as possible like a real consumer – with real consumer information. This includes establishing and gradually increasing good credit in order to optimize fraud gains over time, as well as to build towards obtaining higher end goods. Such fraudsters may begin by applying for credit with a credit card issuer; while it will be declined based on no credit history at that point, a new credit file will have been established based on the initial request. This allows the synthetic identity fraudster to apply for credit again through another lender or subscribe to services that allow him / her to establish a good credit report.

"They put a lot of years into building up a credit report and all that sort of stuff. I don't know how much information they need to truly create a synthetic identity, but I think all that information is out there." *(Director of Accounts, Telecom Services Provider)*

The Threat of Identity Fraud

Since fraudsters are experts at maneuvering every which way to score a win, synthetic identities can be created in various ways to meet fraudsters' needs, including by information from:

Multiple real persons into a single fake identity, with a valid shipping address, Social Security Number (SSN), date of birth, name, etc. – none of which matches any one person. This type may be used for shorter-term fraud gains, such as bigger ticket items.

One real person by using some of his / her information combined with fake data. In this case, the fraudster is likely to be nurturing this identity, using it to establish a good credit history before ultimately "going bad".

No known persons in which the personally identifiable information doesn't belong to any consumer. It is entirely fabricated based on a new SSN, using the same range as the Social Security Administration for randomly-issued numbers. This type of synthetic identity may also be nurtured for longer-term gain and is useful when posing as an underbanked consumer with a less established purchasing footprint (i.e., younger Millennials).

Communications and Media Services companies are particularly appealing to synthetic identity fraudsters.

Fraud executives we spoke with in these companies reported seeing an increase in this type of identity fraud during the past few years. In fact, it was said that it is more prevalent than the use of stolen identities. A key reason is that the subscription-based model of Communications and Media Services companies provides a monthly format to build credit on relatively smaller sums of money. And where a subscription involves devices (phones, satellite dishes, game consoles, cable modems, etc.), there is opportunity for fraudsters to acquire extra devices or equipment and sell them for a profit – which is made easier when fraudsters can apply for family plans.

While Communications and Media Services companies are targets, they may also be the gateway to other fraudulent activity in other industries that have higher value targets. Established credit can lead to larger ticket loans, such as for automobiles, higher end appliances and other valuables that can be obtained and sold for even higher profits before credit limits are maxed out.

The Identity Dilemna

The very nature of synthetic identity fraud makes it extremely difficult to detect before damage is incurred.

A number of Communications and Media Services executives described synthetic identity fraud as being very sophisticated in terms of its approach and conducted by very professional criminals. It's extremely insidious in nature as fraudsters take a longer-term view to developing an established profile little-by-little.

As professionals, synthetic identity fraudsters understand the types of information they need to know in order to gain approval and pass certain checkpoints in the onboarding process. They know how to get through credit checks by knowing what information has to match; further, credit bureau checks are often more about the ability to pay than about identity.

Compared to stolen identities, synthetic ones do not generate a fraud victim in the short term. It's not until much later, when all credit has been maxed out and payment stops, that creditors will turn to the real victim whose partial data was used for fraud. This, in and of itself, makes synthetic identity fraud more lucrative and less risky to the fraudster because it can continue for a longer period of time undetected. In fact, some fraud executives told us that it's hard to quantify the level of synthetic identity losses because it's hard to detect and track.

"With our existing customer accounts, I can keep bad people out. With a sophisticated enough fraudster, if they really do their homework . . . if they've got all the details when I'm onboarding them, then **I don't know that there's much I can do at all to truly establish who they are**." *(Manager of Credit Fraud, Broadband Cable Provider)*

"Synthetic identity fraud is a hard one for me. You're not always sure if someone is using a synthetic identity successfully. I like to measure things pretty tightly, and **this one's a tough one to track**. You kind of have to measure it by proxy and say, "Okay, what's out there that never paid me a dime and I did not classify it as – I did not confirm that it was fraud?" *(Sr. Director, Financial Services, National Wireless Provider)*

The Identity Dilemna

Identity fraud is an issue in both the remote and face-to-face channels.

One might assume that identity fraud is more of a remote (online, mobile) channel issue than it is for the face-to-face / in-store channel. But, that's not necessarily the case. It depends on the transaction, with each channel registering its own set of challenges.

Anonymity creates risk for remote channel fraud throughout the customer lifecycle. Card-not-present, online and mobile channels have become greater targets since the implementation of EMV / chip technology at many physical points of sale. With Communications and Media Services companies, fraudsters take advantage of online onboarding, in which they obtain new services or devices via newly established but fraudulent accounts. They also take advantage of remote channel anonymity to hack existing customer accounts – resulting in the ordering of more devices or services for either their own use or to support criminal activities.

As a self-service channel, the ability to add devices and services makes this approach appealing to fraudsters. New devices can be activated by the subscriber upon delivery rather than at the time of online transaction, which is convenient for fraudsters who actually don't wish to have them activated but rather delivered and sold for profit.

And, the expected online convenience factor works to fraudsters' advantage as well. Consumers expect faster service online. The nature of purchasing and downloading digital goods (music, videos, etc.) tends to involve fast transactions, such that time is of the essence for validating an identity. Without real-time transaction verification, the risk for "fast fraud" increases.

As mobile transactions become more commonplace, these and other challenges will continue. The very nature of mobility makes it difficult to determine location and device profile if using traditional identity verification checks. With mobile transactions, there is need to focus on both the user and the device.

"In most cases, what we are doing is loaning out gaming devices – which may never get activated. **So a lot of the challenges are just keeping the bad guys away from the site.**" *(Credit Fraud Strategy Director, National Wireless Provider)*

"We have high risk in our faceless channels, from new account acquisition to hacking existing customers with adding lines. And we have experienced more this past year." *(Vice President, Customer Experience, Broadband Provider)*

"We do device fingerprinting when you're coming through our web channel, which creates a unique identity for a device. So when it comes back on our network we can say, **"this has been associated with a fraudulent account**." *(Director of Fraud & Abuse, Internet & Telecom Services Provider)*

The Identity Dilemna

With in-store transactions, either for onboarding or adding additional devices / services, time and customer friction are key challenges. While quicker digital goods transactions can be a remote channel issue, there is generally a 12 – 24 hour buffer between an online / mobile transaction and the shipping of physical goods (enough time to validate and remove fraudulent orders for goods such as new mobile phones or modems). But for the in-store channel, this window is less than 1 hour. Sales agents need to follow processes without profiling; behind-the-scenes fraud teams need to correctly distinguish fraud from non-fraud; and, balancing fraud protection with customer friction can risk the loss of legitimate business. This gets even trickier when trying to limit credit "muling" fraud without undue profiling.

These issues get further heightened when the online and physical channels overlap – meaning that a fraudster orders online and then requests an in-store pick-up. Using different channels with different persons (one to order online, another to verify delivery by phone and yet another to pick-up in-person) helps fraudsters evade certain machine-learning triggers – especially with the rise of botnet fraud. They also rely on the hope that in-store reps or fulfillment center staff will be less skilled or interested in fully checking identification documents at pick-up.

"Nobody likes going into a wireless store to activate new service because it can take 45 minutes to an hour to get a new device, even with the same carrier. We don't want to add time and friction to it because it's super competitive and they'll just go somewhere else." *(Sr. Director, Financial Services, National Wireless Provider)*

"I can place an order online and sit there in my own home and do a spoofed IP address, and then I create 20 of them and one of them gets through, and I've got a guy that's going to go down the street – right? – "Go to the store. It's ready. Go pick it up now." (*Director, Customer Journey, Broadband Cable Provider)*

"There's a lot of training required to counter online purchasing to in-store pickup. Some reps are not going to know the difference if an ID is legit or not. That's not in their nature." *(Process Improvement Manager/Risk, Telecom Services Provider)*

Identity Fraud Impact on the Organization

Getting it wrong has consequences.

With identity verification comes the challenge of balancing risk protection against customer friction. Many companies, including Communications and Media Services ones, have only limited information (if any) about prospects – and sometimes limited data about customers as well. Certain groups, including Millennials, can be particularly wary of providing any more personally identifiable information (PII) than is absolutely necessary. As a result, companies must either risk losing a legitimate applicant that feels too uncomfortable with PII requests or rely on third party sources for data and analytics to make the process as transparent as possible.

Since Millennials are a key target market for Communications & Media services, this can become a real challenge for these companies. A 2016 LexisNexis® Risk Solutions study with Millennials found that this segment places limits around the type of PII they are comfortable sharing, will terminate an application session if too many questions are asked of them or if the process takes too long, and has only some trust in providing such information to Communications and Media Services companies.

But Communications & Media Services companies do use various external data sources and tools to detect identity fraud. A common approach is checking identities against credit bureau data to match personally identifiable information. There is also use of risk management providers with solutions that can check / match PII as well.

However, even with these sources and solutions, keeping the "bad guys" out continues to be a challenge, particularly with the sophistication of synthetic identities. Since these identities use some part of real information by professional fraudsters who are knowledgeable about which data is needed to pass identity checks, reliance on credit information and matching of certain personally identifiable information is not enough to detect this fraud.

Identity Fraud Impact on the Organization

Issues with Current Data Sources & Tools for Identity Verification

Fraud executives point to a number of challenges with their current data sources and tools including: data gaps that weaken the ability to find strong matches across aliases or legitimate customers; less user-friendly verification-based questions that even confuse legitimate customers; less than accurate risk scoring / alerts; reliance on multiple data sources; and all within a limited decision time. This leads to higher false positives, increased customer friction, increased costs and increased risk to the business and customers.

The consequences can be lost business and damaged brand reputation, particularly where victims announce displeasure on Social Media. Those are opportunity costs. But there's also financial loss and **the cost of fraud**, which consists of more than just reimbursing customers or writing-off bad debt. The cost of fraud also involves expenses associated with merchandise replacement / redistribution (i.e., lost devices) and fees if payments are accepted based on stolen or fraudulent credit cards. As a result, this has a multiplying effect for every one instance of fraud losses.

"If the basic is you've got to show ID and provide your basic information, anything you do more than that adds time and hassle to the process. So, you want to do it as infrequently as possible, as targeted as possible. We don't want to add time and friction to it because it's super competitive and they'll just go somewhere else." *(Director of Accounts, Telecom Services Provider)*

"The volume of false positives prevent us from using all the information we might have – it makes us have to operate more loosely than we'd like. But if we flagged or prevented an activation from occurring just because some of these rules were being provided, we wouldn't have too many customers, quite honestly." *(Director of Fraud & Abuse, Internet & Telecom Services Provider)*

Effective Solution Layering to Identify Fraud

New threats require new ways of attacking them.

Newer forms of fraud, coupled with newer transaction channels and payment types, means that traditional solutions and approaches may not effectively detect identity fraud – particularly within the multi-media / multi-channel Communications and Media Services sector. Identity verification challenges differ by channel; technology, security and risk issues differ between using online or mobile browsing and devices; synthetic identities cause confusion by using lots of real information. As a result, there is no single solution. It is important to invest in different solutions that uniquely address specific transaction risks, rather than the same solution(s) for addressing all in the same manner; otherwise, fraudsters will seek out and take advantage of the gaps.

When thinking about multiple solutions, it's not necessarily about the number as it is the effective layering of both identity and transaction verification tools that protect against each of the potential entry or weak points for fraudsters. For example,

- **Protection by Channel:** ID verification via a government-issued ID is important for in-store transactions; geolocation and device fingerprinting are important for remote channel identity verification; and quiz/knowledge-based authentication are extra levels of protection across channels;
- **Protection by Transaction:** real-time transaction verification is critical for protecting against fast fraud with digital services; red-flag rules are important to provide more accurate alerts, thereby reducing false positives and friction – not every transaction can be a priority;
- **Protection by Payment Methods:** adding a layer of protection with credit/debit card payments is particularly important for transactions going through remote card-not-present channels.

The above involve both identity and transaction verification solutions. Both perspectives are important in order to close the gaps that fraudsters will exploit.

- **Identity verification** is important for letting your customers in with the least amount of friction and risk.
- **Transaction verification** is important for keeping the "bad guys out".

Fraudsters are skilled and constantly evolving. Communications and Media Services companies need a dynamic, multi-dimensional arsenal to protect themselves and their legitimate customers.

Effective Solution Layering to Identify Fraud

LexisNexis® Risk Solutions can help.

LexisNexis® Risk Solutions provides powerful identity verification, identity authentication and transaction scoring tools to combat fraud, along with an integrative platform that enables multi-layered solutions to interact with each other for maximum fraud protection. These solutions can help to:

Identity Verification

- Validate name, address and phone information
- Reconcile name variations, duplicates, multiple addresses, and myriad other inconsistencies and linkages
- Perform global identity checks with seamless integration and reporting capabilities

Transaction Risk Scoring

- Quickly detect fraud patterns and isolate high-risk transactions, particularly those involving synthetic identities
- Resolve false-positive and Address Verification Systems failure
- Identify risks associated with shipping expensive goods through risk scoring delivery details

Deep Research Support

- Access billions of data records on consumers and businesses
- Discover linkages between people, businesses and assets
- Leverage specialized tools for due diligence, account management and compliance

Identity Authentication

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

Let us help protect you against identity fraud

With sound customer data management and world-class predictive analytics, LexisNexis® Risk Solutions can help you stay ahead of evolving fraud tactics and ensure that the person on the other end of the transaction isn't a fraudster—without sacrificing a legitimate customer's experience. Tap into our unparalleled breadth and depth of consumer and alternative data — composed from 45 billion consumer records and more than 10,000 sources — for robust consumer insight and a more complete view of risk.

For more information, call 1.800.869.0751

or visit lexisnexis.com/communications

LexisNexis® RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict, and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information and analytics for professional and business customers across industries.