

WHITE PAPER

How Identity Mitigates Risk

TABLE OF CONTENTS

Introduction	03
Where Risk and Identity Overlap	04
How to Mitigate Risk With Identity	06
How Neustar Can Help	07
About Neustar	08

INTRODUCTION

The COVID-19 pandemic [accelerated the adoption](#) of remote interactions and transactions between consumers and organizations. To mitigate risk in these remote connections, organizations need confidence in users' identities.

Identity plays an essential role in diverse business functions, from fraud prevention to contact centers to compliance. Where many organizations segregate these functions, Neustar, a TransUnion company, sees them as parts of the same whole, all driven by consumer identity.

Most organizations operate with an incomplete understanding of users' identities, increasing risk of identity fraud, frustrated customers, operational waste, or regulatory violations. The uncertainty degrades organizations' authentication experiences, outbound communications operational efficiency, and compliance posture. These liabilities cost organizations [millions](#) in identity fraud, [inefficient operations](#), and [regulatory fines](#) and class-action lawsuits.

Most organizations operate with an incomplete understanding of users' identities, increasing risk without potential for reward.

WHERE RISK AND IDENTITY OVERLAP

Fraud Prevention

In the past, [knowledge-based authentication](#) (KBA) challenge questions and [one-time passwords](#) (OTP) sent over automated calls, SMS text messages, or email were sufficient for authenticating inbound callers and digital users. Today, these legacy authentication methods are vulnerable to identity fraud such as account takeover (ATO) because they [hinge](#) on attributes of consumers' identities that have been compromised. Personally identifying information (PII), the answers to KBA challenge questions, has been [breached and divulged](#) on social media for years. Likewise, [email accounts](#) and [phone numbers](#), once useful signals on their own, are not nearly as powerful or reliable without additional [datapoints](#) for [corroboration](#). The most widely adopted digital authentication solutions fail to address emerging fraud vectors because they [narrowly focus](#) on limited or individual data linkages. Losses due to ATO rose [50 percent](#) between 2018 and 2020, costing brands over \$1,300 per incident on average.

Consumers hold brands [responsible](#) for protecting their accounts, but efforts to [shore up](#) legacy authentication processes should not degrade customer experience. Authentication [sets the tone](#) for customers' [feelings](#) toward brands. As [noted](#) by McKinsey, "More than any other aspect of a customer's journey, 'failing to authenticate' drives down customer satisfaction and overall brand perceptions." Leading brands' [investments](#) in smoother, more secure digital

authentication experiences [increase pressure](#) to improve customer experience for phone-channel authentication.

Brands that fail to implement more user-friendly authentication experiences are increasingly likely to [lose](#) customers. Over [15 percent](#) of consumers in the United States say they would abandon a beloved brand after just one bad customer experience. Consumers have shown little patience for an analogous mistake in the purchasing process. Almost [40 percent](#) of consumers will abandon a credit card after a false decline.

Legacy authentication processes also squander operational efficiency. In the contact center, agent-driven KBA takes 30 to 90 seconds, adding an average \$0.45 to \$0.90 to the beginning of each applicable call. Over [80 percent](#) of contact centers rely on agents as the first line of defense in identifying potential fraud. Online, one-size-fits-all authentication approaches errantly flag some customers and transactions as suspicious (i.e. false positives) and add to a manual review queue unnecessarily. This undercuts the efficiency gains of digital interactions.

An incomplete understanding of identity degrades the value of authentication. It enables fraudsters, frustrates customers, and hinders operational efficiency. And the fundamental nature of the problem is not limited to inbound channels.

Contact Centers

Outbound communications organizations live and die by their right-party-contact (RPC) rates. Missed connections mean costs without revenue.

RPC rates are often a function of the accuracy of compiled credit bureau and demographic information. This type of customer intelligence has [little value](#) for outbound communications activities: consumers' credit risk and behavior, and Know-Your-Customer identifiers, such as dates of birth and social security numbers. Traditional sources of consumer data lack insight into identifiers that have the most influence on RPC rates: a "contactability score" for each consumer, the most active phone number among multiple possibilities in a consumer record, and the [times and days](#) when each consumer is most likely to answer her phone.

Conventional consumer data sources also struggle to keep up with the rate at which traditional identifiers change. Up to [fifteen percent](#) of the overall information in a CRM goes out of sync in a single month. A commissioned [study](#) conducted by Forrester Consulting on behalf of Neustar found that over 60 percent of respondents believe resolving "lack of contact data" was "critical" or "important" to addressing challenges in contacting consumers. Nearly half of firms experienced increased operational costs, and 43 percent lost productivity due to these challenges.

However, a correct CRM record is no guarantee that a consumer will answer a call or text. Legitimate communications are regularly [blocked](#) by mistake or incorrectly flagged as spam by call management systems. Five percent of outbound calls are flagged according to Neustar's [Robocall Mitigation](#) carrier deployments. An organization's caller ID may be quite often showing up as blank, inconsistent, or incorrect, which consumers are [less likely to trust](#) enough to answer. Over [80 percent](#) of Americans say they do not answer calls from unknown numbers.

Both consumers and contact centers need confidence in the others' identities for effective and efficient connections. RPC rates languish for lack of that confidence, squandering operational resources. But that's not the extent of the financial risks of operating with an incomplete understanding of identity. Regulations raise the stakes.

Compliance

An incomplete understanding of identity could lead organizations to call consumers [without their consent](#) (a violation of the Telephone Consumer Protection Act (TCPA), make more collection attempts per week than is [allowed](#) under the Consumer Financial Protection Bureau's Regulation F, or misstep in the [verification and resolution](#) of identities subject to the California Consumer Protection Act (CCPA). Unintentional mistakes could lead to significant regulatory fines and class-action damages.

Organizations that choose to operate with an incomplete understanding of identity in these functions—fraud prevention, contact centers, and compliance—accept unnecessary risk. They expose themselves to more fraud loss, incur higher operational costs, and provoke more compliance risk.

Conversely, investing in identity helps mitigate risk across the organization. Knowing as much as possible about the consumer allows organizations to mitigate fraud, improve customer experience, increase efficiency, and comply with regulations.

HOW TO MITIGATE RISK WITH IDENTITY

A complete understanding of identity is the foundation for actionable risk intelligence and competitive advantage. The more that is known about consumers, the more effective and less risky consumer interactions can be.

Identity is at the heart of knowing the user. It is not just a phone number, device ID, or email address. Identity is an [actionable understanding](#) of who or what is on the other end of every interaction and transaction. The sum of a user's identifiers and interactions separates risky transactions for additional verification from customers who should be let through faster. Identity enables organizations to contact the right customer at the right number and right time, and ensures outbound communications are not improperly blocked, mislabeled as spam, or misrepresented on caller ID. It ensures a reliable compliance posture.

If mitigation of the risk vectors described earlier is beyond the capacity of in-house capabilities, invest in an identity-driven risk solution that uses real-time intelligence to support effective decisions. The goal is a single, 360° view of each consumer, so organizations can build trust by efficiently connecting with customers, while mitigating fraud and compliance risk.



360° VIEW OF CONSUMER

HOW NEUSTAR CAN HELP

[Neustar TRUSTID Solutions](#) uniquely delivers on the promise of complete identity resolution: [blocking](#) out fraudsters and letting customers through faster, [improving](#) the contact center's bottom line, and [mitigating](#) compliance risk. These disparate use cases share a common need to connect across people, location, and device data. The [Neustar OneID®](#) platform makes all of the above possible.

OneID leverages advanced data science, probabilistic and deterministic graphs, and proprietary third-party data enhancement to create a complete, accurate, and persistent view of identity. It houses consumer and device identity data that is updated and corroborated over two million times daily from over 200 authoritative sources for an exceptionally high degree of trust. An always-on network of partners, including all major phone carriers, provide constantly updated consumer attributes and device ID linkages, combining online, offline, and device-based data for unparalleled accuracy and reliability. Industry-leading privacy measures and data protection standards safeguard all this data in accordance with [Neustar's privacy principles](#), contractual obligations, and applicable data privacy laws.

All Neustar business units' solutions draw on OneID's identity service, and their exhaust enriches the platform's data and intelligence in real time. [Marketing](#) connects online identities to consumers offline by harnessing hundreds of millions of IP addresses, device IDs, and email addresses. [Security](#) delivers authoritative decisioning data on 99.99 percent of the world's routable IP addresses and handles over one trillion DNS queries per month. [Communications](#) powers over 90 percent of caller ID in the U.S., yielding MNO carrier device data on over 500 million landline and mobile phones. These high volumes of data enter OneID for transformation, normalization, and analysis, becoming insights and recommendations that solve large and persistent problems across industries.

Multiple companies excel in either people, location, or device data. Only Neustar links all three in a consistent and highly accurate fashion. This unique view of identity is how [Neustar TRUSTID Solutions](#) help companies build trust by efficiently connecting with customers, while mitigating fraud and compliance risk.

LEARN MORE

For more information, call **1-855-898-0036 x4**, email **risk@team.neustar**, or visit **www.risk.neustar**

ABOUT TRANSUNION (NYSE: TRU)

TransUnion is a global information and insights company that makes trust possible in the modern economy. We do this by providing an actionable picture of each person so they can be reliably represented in the marketplace. As a result, businesses and consumers can transact with confidence and achieve great things. We call this Information for Good®. A leading presence in more than 30 countries across five continents, TransUnion provides solutions that help create economic opportunity, great experiences, and personal empowerment for hundreds of millions of people.

www.transunion.com

ABOUT NEUSTAR

Neustar, a TransUnion company, is a leader in identity resolution providing the data and technology that enable trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in marketing, risk and communications that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Learn how your company can benefit from the power of trusted connections.

www.home.neustar