DIGITAL IDENTITY:

# Identifying Devices to Prevent Retail Fraud

neustar
A TransUnion® Company

RETAILDIVE

Custom content for Neustar by studioID

# Introduction

Preventing fraud is a real issue for retailers, but in many cases, those efforts are damaging their reputation with customers, and even costing legitimate sales. When legitimate credit card transactions and new customers onboarding are incorrectly tagged as potentially fraudulent, it creates a disappointing consumer experience, adds extra steps to completing the sale, and increases the likelihood customers will abandon the processes and buy somewhere else.

Retailers want happy customers, and happy customers are ones who have minimal friction in their buying experiences. Companies still relying primarily on knowledge-based authentication (KBA) and personally identifiable information (PII) to assess fraud risk, however, are less likely to achieve that goal. Not only are KBA answers easy for fraudsters to find and exploit, but the process also interrogates a consumer about their own identity, which many find intrusive and alienating. Instead, these retailers could be using behavioral-related data to minimize false positives while reducing the time spent validating new accounts and credit card transactions.

More precise fraud detection and less time spent on interrogating identity helps create the frictionless experience customers want. It also increases overall customer satisfaction and makes it more likely they'll return in the future for more sales.

**THE PROBLEM:**

# Knowledge-based Authentication, by Itself, is Highly Vulnerable

A layered approach to authentication may effectively use KBA in certain circumstances, such as transactions or accounts flagged for a higher likelihood of fraud. But relying primarily or exclusively on information people know as the go-to method of authentication puts the burden of collecting data on customers and comes with potential pitfalls. Knowledge-based data is often easy to harvest or guess, making it less effective at preventing fraud. Its limited reliability also — ironically — leads to treating legitimate transactions as fraudulent.

In fact, it's so unreliable that the **false positive rate is some 400% higher** than actual fraud transactions.

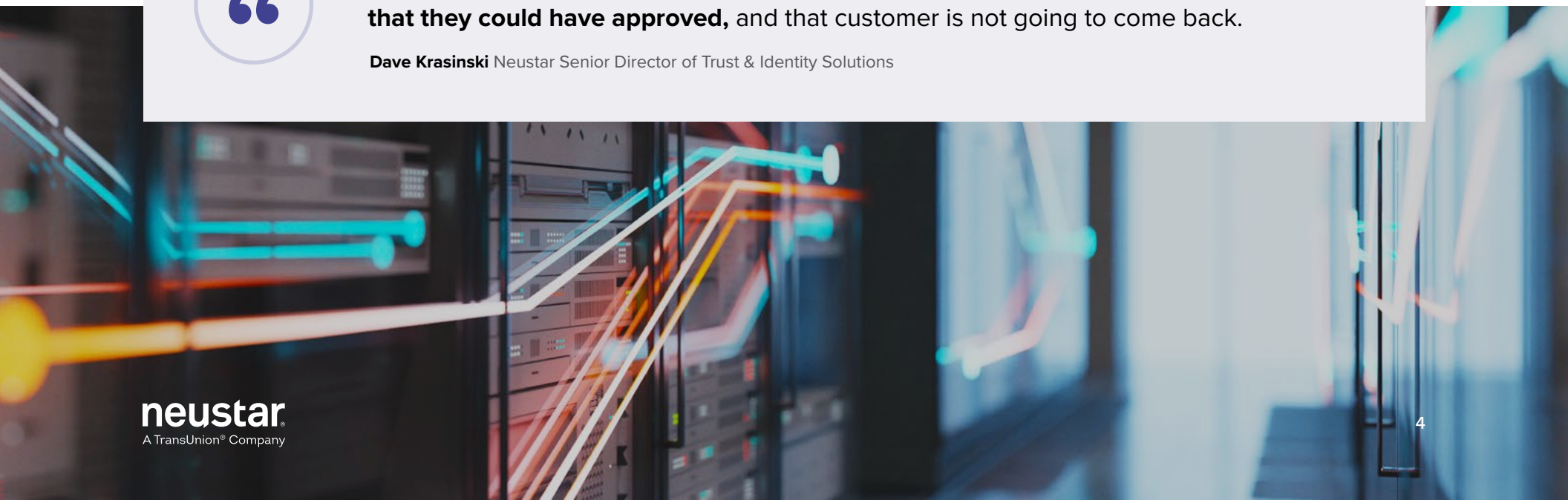
Another part of the problem lies in asking customers to provide pieces of information they may not remember, or that can be easily guessed or harvested by fraudsters. Information like your mother's maiden name, the street you grew up on, and schools you attended are fairly simple to find online.

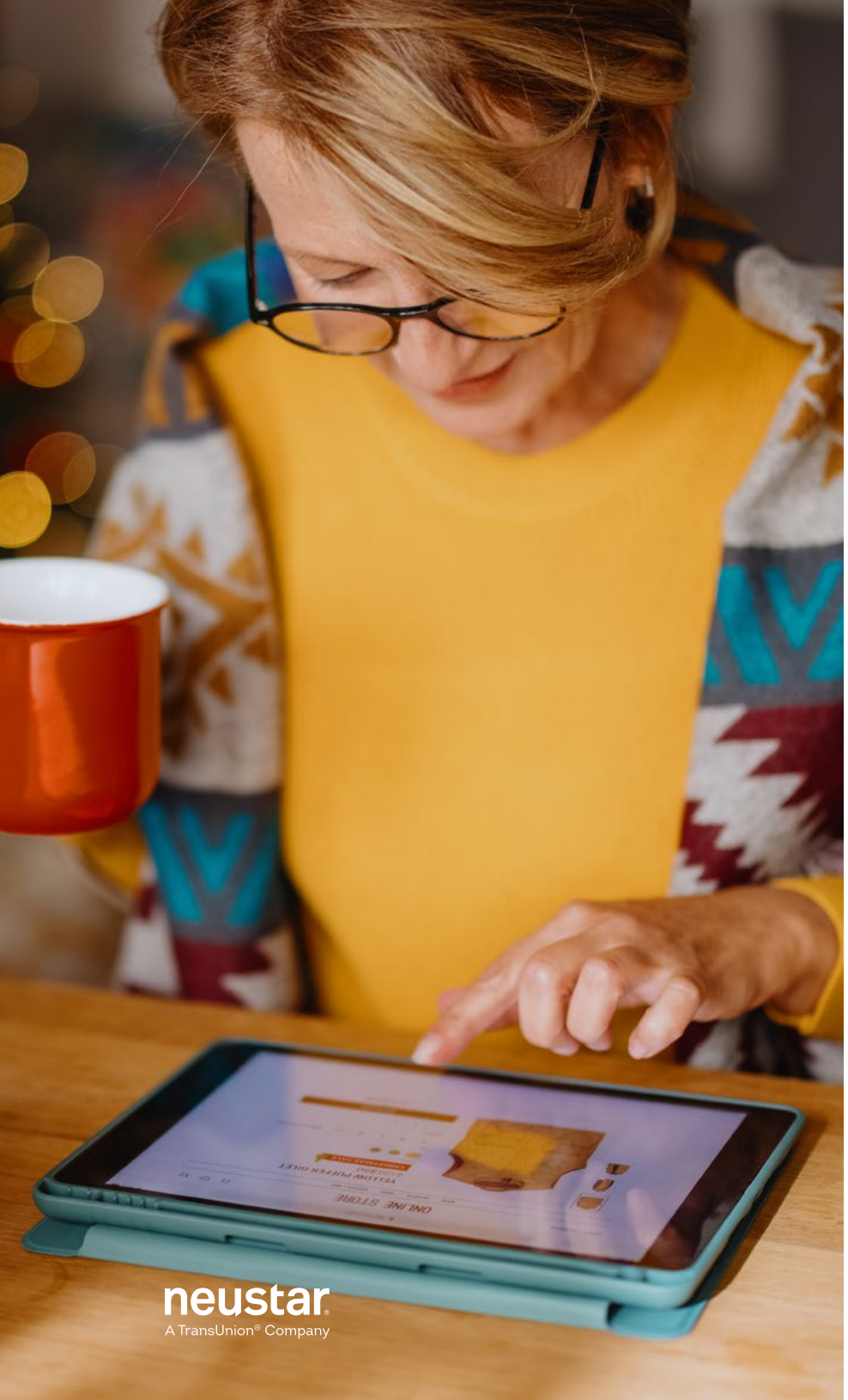
Social engineering is a common way for attackers to trick victims into giving up the information they need to circumvent fraud checks and appear as if they're legitimately making purchases. Social media posts, for example, are often used to collect PII corresponding with customer account verification questions. Social media posts and quizzes asking for pet names are common, as are schemes asking viewers to share their "rock star name," which is a combination of their mother's maiden name and the street they grew up on.

PII is frequently leaked and sold from data breaches, too. Passwords, Social Security Numbers, answers to "secret questions," credit card numbers, previous addresses — all bits of data commonly used to verify customer accounts — routinely show up in retail company data breaches. When shared or sold online, that information can be used to take over legit accounts or create new "synthetic" accounts.

KBA is not only hard to keep out of unauthorized hands, but it also can be difficult for legitimate users to remember. A previous address or phone number, for example, is something that's easy to forget, and requiring this data adds unnecessary frustration to what should be a simple and low-friction purchase process.

> If a retailer has a good customer as a fraudster, or **rejects their order because 'on paper' they look too risky, they're obviously not going to get the money for the transaction that they could have approved,** and that customer is not going to come back.
>
> **Dave Krasinski** Neustar Senior Director of Trust & Identity Solutions






THE SOLUTION:

# Behavioral and Device Data for Frictionless Authentication

Behavioral data, especially when combined with online and offline identity data, is more useful and reliable because it includes multiple data points and is much harder to fake. Instead of focusing on information customers know, behavioral data looks at the patterns and consistency in user activity and devices. Since consumers tend to use the same habits for their online purchases, it's easier to build reliable profiles and harder for fraudsters to work around.

Building a behavioral data profile is a much lower friction experience for consumers and retailers. Instead of focusing on what (asking users to enter information and answer questions), it focuses on how (building a profile based on their devices and activity).

Behavioral data relies on multiple authentication points, such as device data, offline data, and digital data. Since customers tend to use the same devices for online purchases, a different device, like a new smartphone or SIM card, can potentially be a suspicious activity indicator. A change in the email address associated with transactions is another indicator, too. Has the phone number linked to the customer changed? That's another data point that can be flagged.

> Using the **phone's accelerometer to determine how quickly you move the phone, and when you actually start typing,** are examples of sensors helping confirm who you are. **You can get someone's location from the GPS sensor,** and use other characteristics of the phone, too.
>
> **Andrew Chan** Neustar Head of Product Management for Fraud Detection and Prevention

Devices include data that's nearly impossible for fraudsters to mimic. How someone uses their smartphone, for example, can be used with other data points to help determine if they're who they claim to be.

Online shoppers often make their purchases in the same general area, like at home. Seeing a transaction that's far outside their usual shopping area, like a different country, is another potential fraud indicator.

A single change in customer behavior, however, doesn't necessarily mean the transaction or account is fraudulent. Instead, it's another point in the bigger picture. Looking at all the information surrounding a transaction helps determine the likelihood of fraud. A shopper who typically makes purchases from their desktop computer but is using a smartphone instead, is itself not necessarily a sign of fraudulent activity. If the transaction is also happening on a smartphone with a new SIM card in a different country, however, that likely warrants additional verification before completing the purchase.

Using a combination of data that's much more difficult to spoof or steal, and doesn't rely on users providing information that might be inaccurate or forgotten, significantly lowers the false positive and false decline rates. Real fraud cases are more likely to be caught, too. By more accurately identifying actual fraud, Neustar has helped companies reduce fraud-related losses by 20%, saving potentially millions of dollars annually.

"Part of the challenge with KBA questions is that they're just a bad experience in general. Those questions are information a good fraudster can figure out pretty quickly, and it's data that's available by some Google searching," Krasinksi said. "What we provide is more secure and trustworthy information. A fraudster — no matter how good they are or how well funded their frauding is — can't fake the data we check."

More accurate fraud detection also helps create the frictionless purchase experience customers and retailers want. Fewer false positives mean more satisfied customers, since the number of transactions requiring additional verification is much lower. For retailers, that equates to happier customers who are more likely to return and make additional purchases.

Fraud detection is tricky because it isn't just about stopping losses. It's also about the impact on users and user experience. Creating a friction-right buying experience is important for the customer, retailer, and credit card issuer.

Instead of relying exclusively on KBA to identify fraud, **Neustar's more encompassing behavioral and device validation solutions are more reliable, give substantially fewer false positives, and lead to lower customer frustration,** which ultimately saves money — a win for everyone.


neustar®
A TransUnion® Company
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.
LEARN MORE


## BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

**LEARN MORE**