neustar
A TransUnion® Company

Whose Credit Line Is It Anyway?

The Growing Problem of Account Origination Fraud (and What You Can Do to Stop It)

Table of Contents

Executive Summary

Account origination fraud—that is, opening a credit or bank account with fraudulent or falsified information—costs the banking industry, businesses and consumers billions of dollars each year. Despite the myriad of safeguards in place, banks are more exposed to fraud than ever before, due in part to the growing number of channels customers use to access financial institutions, such as e-banking and mobile apps. In an effort to assess and address the problem of account origination fraud, Neustar and American Banker recently conducted an in-depth research study of more than 200 U.S. banking executives to find out how big the problem really is, and what organizations are doing to protect their business and their customers from fraud.

The Research

This research study was conducted online during June 2016. The research group featured 207 senior-level financial executives who rated their involvement in their organization's fraud, risk and compliance processes as moderate to high. Each of the participants was a member of American Banker's opt-in subscriber base at the time of the research.

The Goal

The goal of the research was to shine a light on industry challenges and best practices as they relate to account origination fraud. Within that aim were four distinct subgoals:

- **Better understand how account origination fraud impacts organizations**
- **Catalog how organizations address account origination fraud today and how they plan to address it in the future**
- **Identify which needs and challenges remain to address account origination fraud**
- **Outline the solution features that can help organizations effectively combat account origination fraud**

Whose Opinion Is It Anyway?

American Banker and Neustar interviewed 207 senior-level U.S. financial executives to compile this report. Research participants represent a cross-section of the financial industry (see Figure 1).

PARTICIPANT AFFILIATION

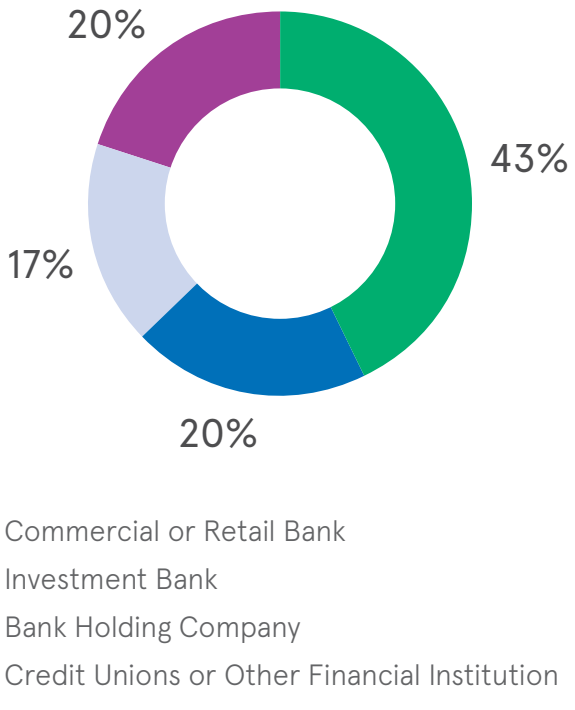

Figure 1. Affiliation of research study participants

The organizations they represent range from medium to very large (see Figure 2).

TOTAL ASSETS UNDER MANAGEMENT

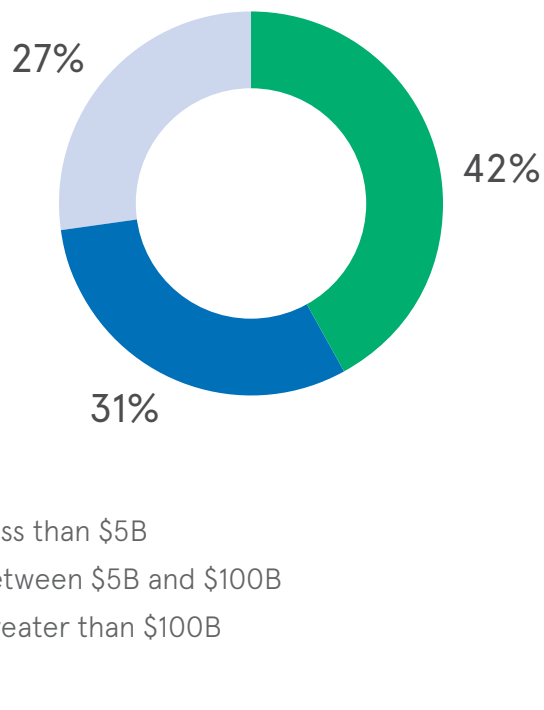

Figure 2. Total assets under management by affiliation

The participants rated themselves as having moderate to high involvement in operational decision-making as it relates to fraud prevention, risk mitigation and industry compliance within their organization. Those who rate themselves as having a high level of involvement outnumber those with moderate involvement by roughly two to one (63% vs. 37%). Their job functions cover a cross-section of business disciplines including finance, IT, risk management, general management and strategy/development planning.

The participants occupy senior roles within their organizations (see Figure 3).

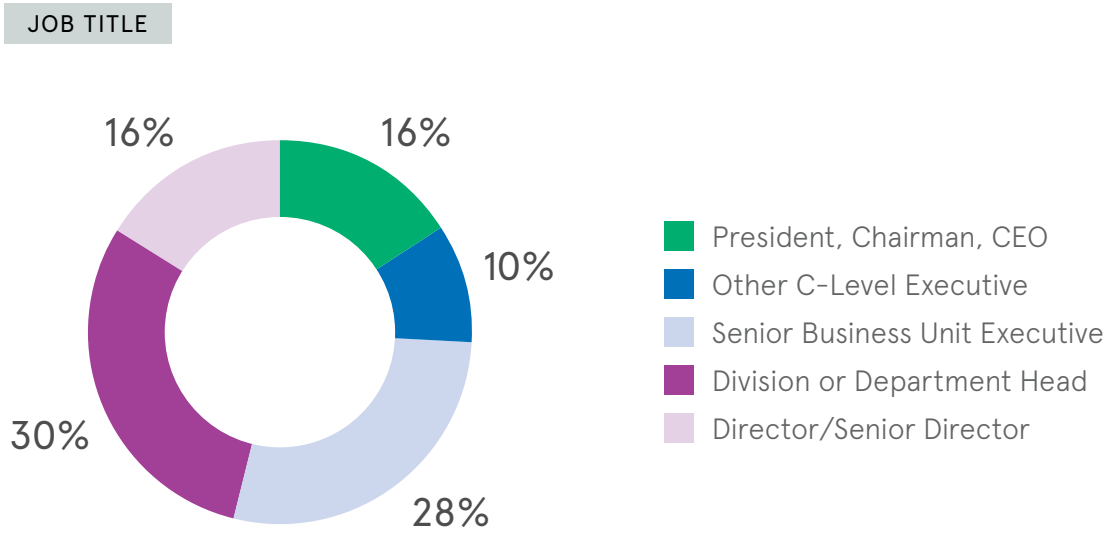

Figure 3. Research study participants by job title

What's the Problem?

Account origination fraud is not a new problem for financial organizations, but it is a growing threat. A recent report from Aite Group confirms that 48% of financial institutions saw an increase in online application fraud from 2013–2015 and 25% reported an increase in mobile application fraud during that same timeframe. In fact, U.S. credit card application fraud alone is projected to grow from $1.1 billion in 2016 to over $2 billion in 2020.[1]

As the fraud threat landscape evolves, financial organizations continue to make fraud detection and prevention a priority, yet fraudsters still manage to steal billions of dollars each year through the creation of fraudulent banking and credit accounts.

Today, two out of three financial organizations (63%) report being negatively impacted by account origination fraud. Affected organizations reported the following impacts to their business due to fraud (see Figure 4).

FRAUD IMPACT

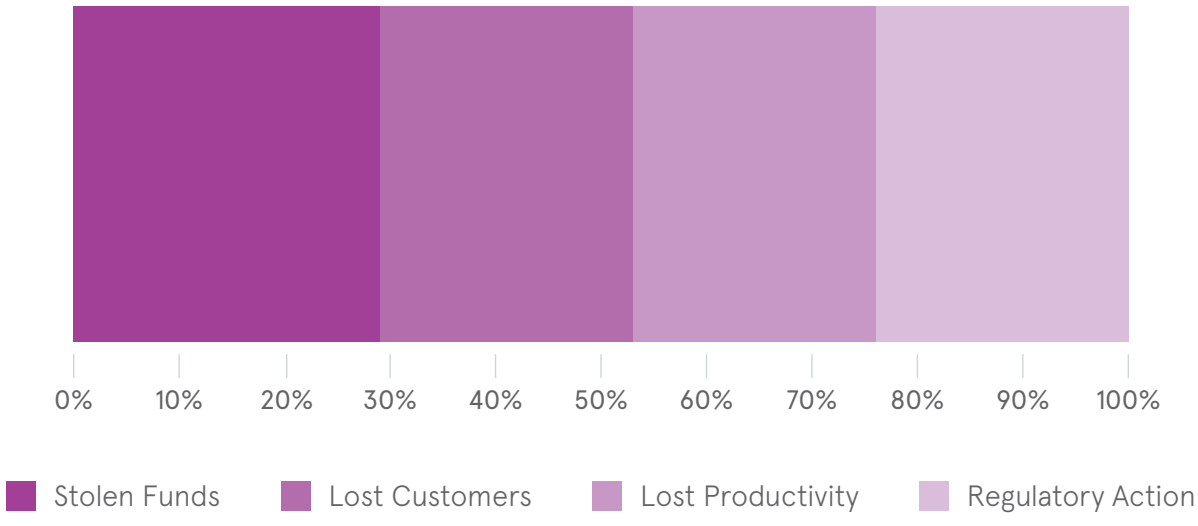

Figure 4. Business impact of account origination fraud

[1]Source: Aite Group, Application Fraud Rising as Breaches Fan the Flames, March 2016

Financial losses incurred as a result of account origination fraud range from substantial—70% report losses of more than $100,000 in the last 12 months—to painful, with one in five (21%) reporting losses of greater than $2 million (see Figure 5).

ACCOUNT ORGINATION FRAUD LOSSES

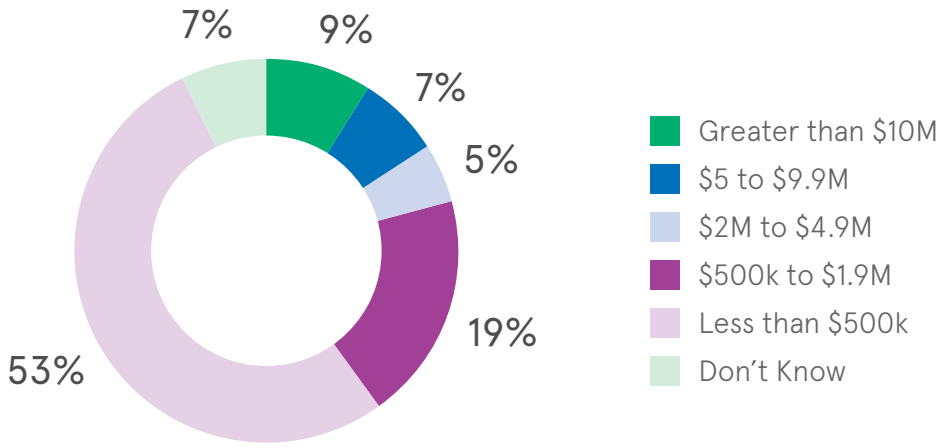

Figure 5. Financial loss caused by account origination fraud

Productivity losses are another significant factor when measuring the true cost of fraud. The American Banker/Neustar research found that organizations spent an average of 24 hours investigating, reporting and following up on each account origination fraud incident, with one in four incidents requiring 3X that amount (76 hours) from investigation to customer communication.

CURRENT AND PROJECTED ACCOUNT ORIGINATION FRAUD RISK IN THE US

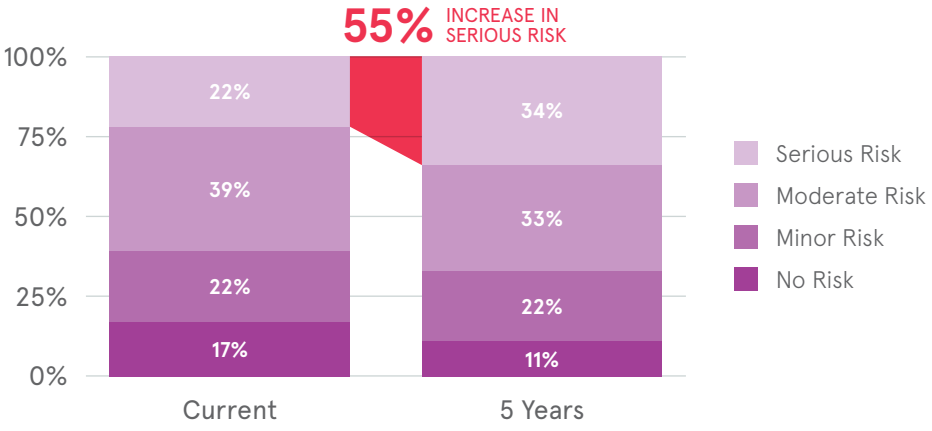

Figure 6. Current and future risk measurements for account origination fraud

The rise in the number of account origination fraud attempts mirrors a growing sentiment among researched executives that account origination fraud will escalate to a serious risk for financial organizations over the next five years. According to the American Banker/Neustar research, one in five senior executives believes that account origination fraud is a serious risk today, but one in three believes it will be a serious risk five years from today (see Figure 6). Not surprisingly, those organizations that have been negatively impacted by account origination fraud in the last 12 months are most likely to perceive it—and other forms of fraudulent activity—as a serious risk in the future.

What Are Organizations Doing about It Today?

Among the financial organizations that were researched, most have fraud detection and identity authentication measures in place to prevent against identity theft and account origination fraud. The median amount spent on fraud prevention, according to the research, was $500,000 per year.

Account transaction monitoring (71%) and traditional identity verification solutions (71%) were the most common preventive measures, followed by digital identity verification (57%). Yet the responses provided by researched executives indicate that gaps exist in these solutions, particularly with regards to protecting those channels executives are most worried about: online and mobile channels.

Despite the growing presence of new digital channels, senior executives still view tried-and-true identity information such as name verification (61%) and address verification (52%) as the strongest attributes for personal identification. Slightly lower in acceptance, but more indicative of the future of digital identities, are personal identification methods such as device ID (43%), email verification (39%) and device location (35%) (see Figure 7).

MOST EFFECTIVE IDENTIFICATION ATTRIBUTES

Figure 7. Most effective identification attributes against fraud

Of course, the critical juncture for authentication and verification is when an account is first opened. More than two-thirds of research respondents (68%) indicated their organization used an identity verification and authentication solution to confirm the account holder's identity at the time of new account creation. Roughly half of those respondents also reported using third-party data (51%), internal customer relationship management (CRM) data (46%) and blacklist services (44%) to confirm identities prior to opening a new account (see Figure 8).

Here again, however, the types of customer data used to confirm identities would seem to favor traditional methods over newer digital forms of identity. Senior executives report that most organizations use government-issued IDs (73%) for identification at account opening, followed by credit reports and consumer credit bureaus (66%), third-party vendor data (52%) and utility bills featuring the customer's address (45%).

METHOD OF IDENTITY VERIFICATION AT ACCOUNT CREATION

Figure 8. Methods of ID verification at the time of account creation

What More Needs to Be Done?

According to the financial organizations we researched, risk mitigation priorities today focus on reducing losses and retaining customers. Regulatory compliance, revenue/value loss prevention and customer satisfaction were cited as their top three priorities, followed by preserving corporate image, preventing business disruption, customer retention and avoiding productivity losses. Importantly, the majority of respondents (79%) say that account origination fraud is at the top of their fraud prevention priorities—more so where organizations have experienced account origination fraud within the last 12 months.

Senior executives recognize that more needs to be done, however. In the last 12 months, executives report combatting fraud through more training, heightened monitoring and new fraud prevention policies. Increased fraud monitoring and technology upgrades are among their top initiatives over the next 12 to 18 months. Of those executives researched who expect their organizations to spend more money on fraud detection in the future, 40% believe that they'll need to spend significantly more (10% or more year over year) on account fraud prevention going forward.

Executives also believe that awareness and education are crucial in the fight against fraud. In identifying their own best practices, they point to education/awareness, multi- and cross-channel verification and biometrics as some of the most effective methods to address account origination fraud now and in the future.

What's the Answer?

When it comes to preventing fraud, financial organizations don't lack for a variety of solutions. What these solutions lack is consistency of implementation. Only 6% of respondents in our research indicated that their organization had a fully integrated fraud solution across their enterprise. The risk of using different and disconnected systems to combat fraud can result in policy and identity gaps that lead to errors, inconsistencies and security breaches.

As part of the research study, financial executives were presented with a description of Neustar's solution for account origination fraud prevention and risk mitigation, but were not told who the vendor was. The solution was described as follows:

> When customers today visit online business, it is difficult to identify and verify customers cross-channel and cross-device. By integrating different silos of identity ecosystems and resolving multiple online and offline identifiers to individuals, we can provide a single view of the identity for customer acquisition, fraud, compliance and risk to enable organizations to build trust and safety in their digital transformation journey. Such a solution not only helps in dealing with authoritative identity resolution of the prospect across all channels, but also helps in linking device and digital endpoints to real identities.

The description then went on to list specific solution features:

- **Verify if identity attributes such as name, address, phone and email match with the user-submitted information**
- **Know the device linked to the identity and the reputation of the device**
- **Link users' online identity and endpoint to authoritative offline identity**
- **Verify users through biometrics of online data linked to real identities**
- **Know the user behind the transaction through user behavioral biometrics**
- **Know the real-time user location (IP and phone location)**
- **Rate risk factors around the identity attributes: phone, email, IP, address, devices**
- **Leverage trusted offline identity data to build identity reputation**

When surveyed, nearly half of all research participants (45%) indicated that they were aware of such a solution, but were unaware of which vendors offered it today (see Figure 9).

AWARENESS OF IDENTIFY VERIFICATION SOLUTION AVAILABILITY

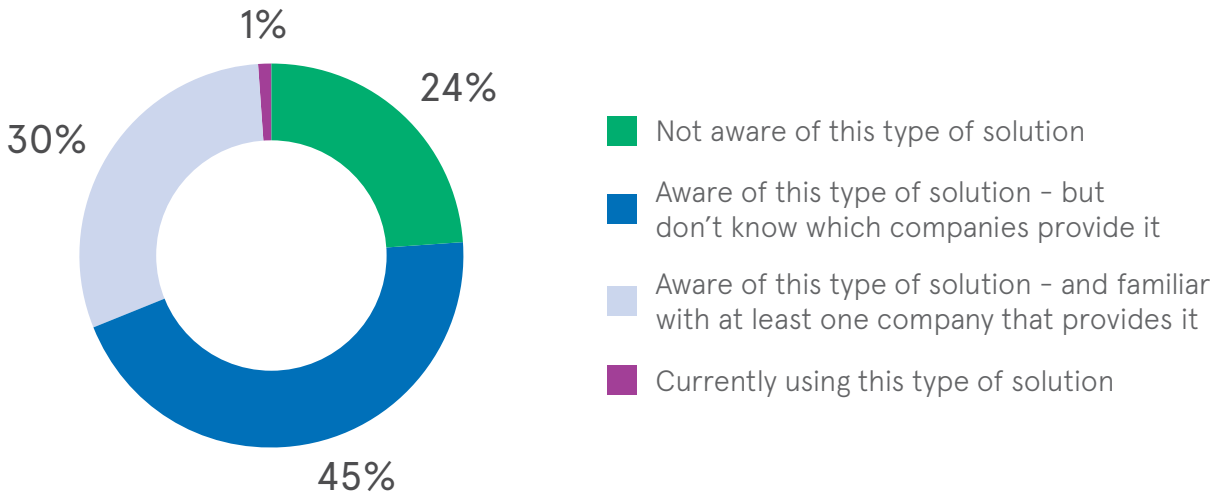

Figure 9. Study response to awareness of the Neustar fraud solution

Study participants agreed that the fraud solution, as described, could help them reduce fraud risk, improve customer experiences and increase profitability. They rated all of the solution's features as "significant" in the prevention of fraud, selecting the ability to match verifiable identity attributes against user-submitted information as the most significant feature (see Figure 10).

SOLUTION FEATURE SIGNIFICANCE

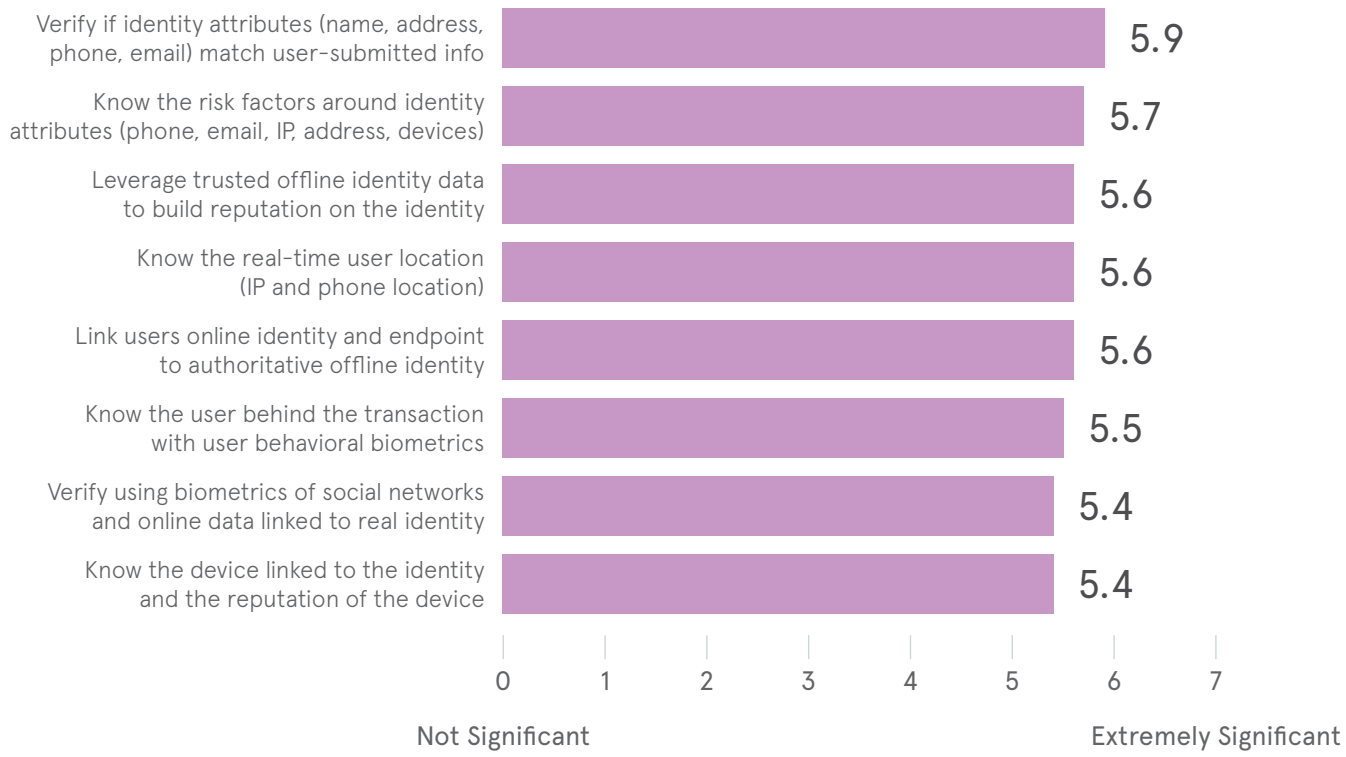

Figure 10. Solution feature significance in the prevention of account origination fraud

The Neustar fraud and risk mitigation solution delivers the capabilities financial organizations have identified as critical to combatting fraud, now and in the future. Neustar provides a fully integrated, enterprise-wide fraud and identity solution that helps organizations reduce account origination fraud, effectively manage risk, ensure compliance and protect customers. Capabilities delivered by the Neustar solution include:

- **Real-time matching of user-submitted attributes with trusted name, address, phone and email information—rated by senior executives as the most important attribute in a fraud solution**
- **Device identification and reputation**
- **Online and behavioral biometrics for identity verification**
- **Real-time location information**
- **Third-party data to create reputation and flag risk of identity attributes**

When presented with how Neustar solutions can help prevent account creation fraud in a "blind" response, research found four out of five senior executives expressed interest in Neustar's capabilities, and two out of three executives said they would be likely to purchase a solution with similar capabilities in the near future.

The Conclusion

Account origination fraud is a big problem that many believe will grow over the next five years. Financial organizations continue to invest in identity and verification solutions to prevent fraud and mitigate risk, yet these measures often fall short, especially when viewed from the vantage point of new attack vectors such as e-banking and mobile apps. Most senior executives agree that the ability to match user-submitted data in real time with authoritative identity information is critical to preventing account origination fraud, yet it should not serve as the only method of authentication. Instead, organizations should use a mix of best practices to identify and authenticate customers including biometrics, device identification, location and third-party data.

Whatever solution an organization chooses, they should implement it consistently across their enterprise to prevent errors, inconsistencies and security "loopholes." In this way, organizations can best detect, prevent and mitigate account origination fraud in their business, while protecting their brand and their customers.

About 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

WP-FRC-50256-01.21.2022