Identifying and preventing synthetic identity fraud

June 19, 2020

While preventing fraud has always been a key challenge for businesses in any industry, the task has been made even more difficult by the prevalence of online sales and the increasing sophistication of fraudsters. As states and localities have imposed restrictions on businesses and consumers have dramatically altered their shopping habits in response to COVID-19, automotive dealers have rapidly embraced online sales and off-site deliveries. While this business model has proved to be a lifeline for many dealers, it also increases the opportunity for fraudsters to use synthetic identities to perpetrate fraud.

Unlike traditional identity fraud wherein the fraudster pretends to be another person and uses their credit, synthetic identity fraud involves the creation of a new identity. This can be done by creating a new fictitious identity from scratch without the use of any personally identifiable information (PII), or by combining real and fake PII to form a new identity.

Typically, fraudsters will build up positive credit history on these identities over time. ID Analytics, a credit and fraud risk analytics company, found that the majority of synthetic identities fell within the "good," "very good," or "excellent" credit-based Fico scoring model categories. Armed with a positive credit history and a good credit score, the fraudster will identify a final target and then "bust-out" to maximize the heist. "Busting out" happens when the fraudster maxes out its credit accounts and ceases payment.

Because many of these synthetic identities use PII and have attractive credit scores and histories, ID Analytics estimates that 85-95% of applicants identified as potential synthetic fraud would not be flagged by traditional fraud models.

For example, the velocity — or how fast an identity seeks credit — has limited impact because unlike traditional identity fraud, the fraudster is in full control over the identity. As such, the fraudster manufactures the identity over time and is not rushed in committing the crime. For that same reason, confirmed negative behavior and past fraud association measures that may be indicative of traditional third party fraud have limited impact in identifying synthetic identities.

Rather than rely on traditional methods for flagging high-risk applications, a dealer may be able to recognize patterns and behavior that are indicative of synthetic fraud. Real people have real history and will often show consistency over time by using the same physical address, email address, or phone records.

Conversely, synthetic identities are often inconsistent or incomplete because while some PII may be real, others are fabricated or non-recurring. If there is doubt about the veracity of an application or identity, consider the following:

Review the individual's history: A review of the types of accounts an individual possesses (or lacks) may raise questions and concerns about the applicant. Consistency and permanency around an individual decreases the chance that an account will misuse credit. For example, if the identity has opened several accounts in various locations within a short period, that may be a sign that the fraudster has simply been cultivating a credit score.

Ask "out-of-wallet" or "challenge questions": Because real people have real history, out-of-wallet questions can trip-up the fraudster and uncover inconsistencies in the application or identity. These questions do not rely on publicly available information and have answers that would be difficult for anyone but the real person to know. For example, though a synthetic identity may contain PII showing a person's current employer, the fraudster might be unable to confirm where the person worked before beginning their current position, or other details related to their employment history. Likewise, a real person would be able to verify their previous addresses where a fraudster might not.

Implement multifactor authentication: As with out-of-wallet questions, using multifactor authentication is based on the premise that fraudsters can't provide the same level of proof as a real customer. Providing customers with a one-time password or code used to confirm their identity is a popular way lenders can strengthen the authentication process. Real people generally use the same phone numbers and email addresses, and requiring the applicant to confirm they have access and ownership of these accounts is an easy way to curb synthetic fraud.

Review bank account data: Often, fraudsters will use stolen or counterfeit payment methods when building the identity's credit and busting-out. Using a vendor or third-party service to review bank account information may uncover inconsistencies within the synthetic identity and reduce the risk that an account is fraudulent.

Incorporate non-traditional data: Non-traditional data, such as phone records or social media accounts, may serve as an additional line of defense. So much of people's lives are online through their social media accounts, and a quick online search may be able to confirm whether the applicant is who they say they are.

As dealers move to online sales and off-site delivery, they should be especially vigilant to guard against synthetic identity fraud.

This article was first published on Auto Finance Excellence, a sister service of Auto Finance News, and is reprinted with permission. McGlinchey is pleased to serve as the official Compliance partner of Auto Finance Excellence, providing insights and thought leadership through webinars, podcasts, and monthly columns.

Related people

Ross Benson