# FraudIQ® Synthetic ID Alerts for auto dealers

When criminals combine pieces of real and fake identities to create a new, fraudulent identity, and use that identity to access money, credit, products or services, it's called synthetic identity fraud. These identities look like real, legitimate consumers, which means they can be nearly impossible for dealers to detect at the time of sale, opening them up to potential chargebacks from their lenders.

It's a pervasive problem for the industry. In fact, a recent analysis shows that while the average loss per synthetic identity fraud incident has remained at $15,000, **total losses from synthetic identity fraud have doubled in the last three years to an estimated $731 million.***

FraudIQ® Synthetic ID Alerts from Equifax help dealerships detect synthetic identity fraud earlier so you can:

- Avoid chargebacks
- Mitigate fraud losses
- Maintain your lender relationships
- Better protect your bottom line

$2.42 billion

A conservative estimate of synthetic identity fraud losses by 2023.

**Aite Group**

Fraudulent synthetic identity accounts that go undetected for 24 months drive estimated **total losses of $200 million per month across all industries — $2 billion annually —** according to a 2021 analysis of the Equifax consumer credit file.*

## Understanding synthetic ID risk levels and next best actions

FraudIQ Synthetic ID Alerts include **Final Risk Assessment Flags** that indicate the likelihood that the input transaction is associated with a synthetic identity. The flags are:

Y = Yes, there is a high likelihood that the transaction is associated with a synthetic identity

N = No, there is not a high likelihood that the transaction is associated with a synthetic identity

U = Undetermined (consumer applicant information is not found)

Also included in the alerts is a **Final Risk Assessment Level (1-5)** which provides a rank-order reference on the riskiness of the alert. Below is an overview of these risk levels, along with potential actions that you can take to efficiently address and remediate the alert.

| Risk type | | Primary action | Secondary action |
|---|---|---|---|
| **Risk level 1** | **Lowest risk** of synthetic identity fraud | Leverage minimal manual verification steps such as utility or phone bill, pay stubs or, if available, use an employment database like The Work Number. | If identity cannot be verified through light touch manual review, you can try phone/ address look ups.<br>– Low risk outcomes can be followed up by SMS to the phone number (secure, multi-factor authentication)<br>– High risk outcomes require manual review |
| **Risk level 2** | **Low to moderate** risk of synthetic identity fraud | | |
| **Risk level 3** | **Moderate risk** of synthetic identity fraud | | |
| **Risk level 4** | **High risk** of synthetic identity fraud | Conduct thorough identity proofing: leverage two (2) residential proof documents (utility statements), phone/email verification, and multi-factor authentication approach or: one (1) government-issued photo ID for document verification with facial recognition. | If there are SSN alerts (shared SSN, invalid or unverified), request customers complete the Social Security Administration's (SSA) form to verify their SSN. |
| **Risk level 5** | **Highest risk** of synthetic identity fraud | Conduct thorough identity proofing with recent utility bills, a recent pay stub, and multi-factor authentication approach with government-issued photo ID for document verification with facial recognition. | If there are SSN alerts (shared SSN, invalid or unverified), request customers complete the SSA's form to verify their SSN. |

## Visit equifax.com/business/identity-fraud or contact your sales representative for more information today.

* Source: Equifax Data and Analytics

Copyright © 2022, Equifax Inc., Atlanta, Georgia. All rights reserved. Equifax is a registered trademark of Equifax Inc. 21-106493