Risk Checklist

Financial Institution

Synthetic Identity Fraud Prevention Checklist

A “synthetic identity" is created using a combination of made-up and stolen information. Fraudsters create false identities to open cards and/or loans to capture funds.

It is especially important to watch for synthetic identity fraud attempts after a major data breach occurs. This checklist highlights steps to help prevent and mitigate synthetic identity fraud.

Allied Solutions

May 2021

Synthetic Identity Fraud Prevention Checklist

- ☐ Use multiple layers of authentication to validate the identity of a consumer requesting to open a card, account, or loan online or in a branch.
- ☐ Request additional identifying information aside from just social security numbers to authenticate a consumer's identity, this can include address, phone number, or other identifying metrics.
- ☐ Advise your consumers to shred/destroy documents with any personal or financial information and to never share these documents with anyone.
- ☐ Educate employees and consumers and advise that they take extra caution when receiving a phone call or email that asks for any personal or financial information.
- ☐ Review the credit reports of new consumers to spot any oddities that may indicate identity theft or synthetic identity theft.
- ☐ Let consumers know they can place a free credit freeze at the credit bureaus to prevent loan or credit requests performed without their consent.
- ☐ Advise that consumers use complex passwords to prevent access to their online accounts.
- ☐ Tell staff and consumers to monitor accounts regularly to spot any unauthorized or suspicious activity.

Visit our website for more risk education: ***alliedsolutions.net/resources***

Contact us to receive more risk education and support: alliedsolutions.net/bond.

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

This checklist is for informational purposes only and is not to be considered legal advice.

975-R5-5.21