700 SW Jackson Street
Suite 803
Topeka, KS 66603

Kansas
Department of Credit Unions

Phone: (785) 296-3021
Fax: (785) 296-6830
kdcu.office@ks.gov
www.kdcu.ks.gov

Jerel Wright, Administrator

Laura Kelly, Governor

**DATE:** **December 2, 2019**

**BULLETIN:** **2019-KDCU-CUB-16**

**TO:** **Kansas Chartered Credit Unions**

**SUBJECT:** **Synthetic Identity Theft**

## SYNTHETIC IDENTITY THEFT

If your credit union has not been victimized by synthetic identity theft, it is only a matter of time. What is "synthetic identity theft"? It is a crime in which criminals combine fictitious and real information to create new identities to defraud financial institutions. In July 2019, the Federal Reserve issued a white paper, *Synthetic Identity Fraud in the U.S. Payment System*, which contained a review of the causes and contributing factors. Obviously, with this bulletin, we step away from regulatory guidance to provide information still related to the safety and soundness of your credit union.

This type of identity theft tends to be more prevalent in the United States because of our dependence on static personally identifiable information (PII), including Social Security numbers. A contributing factor to the problem could be a 2011 decision by the Social Security Administration (SSA) to begin randomly assigning SSN's rather than tying the first three digits to a particular geographical area. Fraudsters will use SSN's from children, the elderly and the homeless – those groups being least likely to notice the fraud in a timely manner. Unfortunately, if a child's SSN is used, by the time it is discovered – when the child is applying for a first car loan – it will take much more time and trouble to remedy. Credit bureaus and financial institutions will assume the first person to use the SSN is the true owner of the number.

In traditional identity theft, a criminal pretends to be another real person and uses his/her credit. How does synthetic identity theft work? The criminal creates a new identity using a variety of methods: a completely fictitious identity without any real PII to a combination of real and fake PII to form a new identity. While the first attempt to obtain credit may be denied, the credit bureau automatically creates a new credit profile since the "applicant" is considered new. If the criminal is persistent, eventually a credit application will be approved as an artificially high credit score has been established. The criminal may attempt to expedite the process by "piggybacking" as an authorized user on to an account with good credit.

Once approved, the criminal can see their credit score artificially rise and secure larger extensions of credit. At that point, the criminal maxes out the credit line and vanishes. In the alternative, identity theft might be claimed first and the balance wrote off. Then, the criminal maxes out again and vanishes for good.

Unfortunately, there are estimates that 85-90% of applicants with synthetic identities were not flagged as high risk by traditional models. One year after application, these individuals had an average past amount due of $8,000.00.

In 2008, the SSA introduced a written Consent Based Social Number Verification (CBSV) service which allows paid subscribers to verify a SSN holder's name and date of birth with written confirmation from the SSN holder. Currently paper-based, the SSA expects to roll out an electronic version in June 2020.

Whatever surveillance method is chosen, credit unions should remain on guard for synthetic identity theft.