

**DATE:** October 19, 2020  
**BULLETIN:** 2020-KDCU-CUB-21  
**TO:** Kansas Chartered Credit Unions  
**SUBJECT:** National Cybersecurity Awareness Month

### NATIONAL CYBERSECURITY AWARENESS MONTH

October is National Cybersecurity Awareness Month and is, therefore, the perfect month to address this critical topic [once again](#). The Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC) have recently issued advisories to increase cybersecurity awareness and assist financial institutions in detecting and reporting fraudulent activity, including ransomware.

FinCEN issued its advisory ([FIN-2020-A006](#)) to provide information on ransomware trends and associated money laundering activities. The information supporting the advisory was compiled from Bank Secrecy Act data and law enforcement partners. “Ransomware” is a form of malicious software – “malware” – designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments in exchange for decrypting information and restoring access to systems or data.

Ransomware is a growing concern for financial institutions because of the role they play in the collection of ransom payments. The process generally requires at least one depository institution and one (or more) money services businesses. The financial institution may be used to purchase cryptocurrency which is then moved on to the criminal holding the account hostage.

These attacks continue to rise and the FBI’s Internet Crime Complaint Center (IC3) reported 2,047 ransomware complaints in 2019, a 37% increase over 2018, with adjusted losses of \$8.9 billion. ([2019 Internet Crime Report](#)) Overall crime statistics in the report showed 1,970 Kansas citizens reported being a victim of internet crime with the total loss exceeding \$16 million. One red flag would be a member asking about cryptocurrency, yet seeming to know nothing about it. The member might be a victim.

The focus of the OFAC [advisory](#) is the sanctions risks associated with facilitating ransomware payments. OFAC has designated numerous cyber actors under its cyber-related sanctions programs, including those who perpetrate ransomware attacks. Facilitating ransomware payments with individuals on OFAC’s Specially Designated Nationals and Blocked Persons List (SDN) is prohibited. This includes country and region embargoes.

OFAC encourages, and financial institutions should already have in place, a risk-based compliance program to mitigate exposure to sanctions-related violations. The program should account for the risk that a ransomware payment may involve a blocked entity or jurisdiction.

Many Kansas credit unions have had members be victimized by internet-related schemes. It is important to be vigilant for the signs of fraudulent activity. [#BeCyberSmart](#) all year long.

**NOTE:** In accordance with Governor Laura Kelly’s [Executive Orders](#) and the [Ad Astra Plan](#), KDCU Administrator Jerel Wright continues to review the feasibility of resuming the on-site examination program. This is being done in coordination with the NCUA.