Compliance eNewsletter

January 8, 2021 Vol. 15, Issue 1

InfoSight News

HAPPY NEW YEAR!

December 2020 Updates

As previously mentioned, 2021 thresholds were updated within the Loans & Leasing Channel topics: **Ability to Repay**, **HMDA** and **HOEPA**. (Note: there were no changes to Credit Card fees or Appraisal limits for 2021.) In the Accounts channel, **Reserve Requirements – Regulation D** was revised to comply with the updated Federal Reserve Requirements.

A new **Risk Alert**, "Prepare for Inclement Weather and the Potential Hazards That Come with It" was also added.

Compliance and Advocacy News & Highlights

NCUA Proposes Amendment of SAR Regs

The National Credit Union Administration Board (NCUA) has issued a notice of proposed rulemaking that would amend the agency's Suspicious Activity Report (SAR) regulation. The proposed regulation would permit the NCUA to issue, on a case-by-case basis, exemptions from SAR filing requirements to federally insured credit unions, when the exemption is consistent with safe and sound practices and can improve the effectiveness and efficiency of Bank Secrecy Act reporting. The proposed rule would also make it possible for the NCUA to grant exemptions, in conjunction with the Financial Crimes Enforcement Network, to federally insured credit unions that develop innovative solutions to meet Bank Secrecy Act requirements.

Comments on the proposed rule will be accepted for 30 days following its publication in the Federal Register, as mentioned in a recent NCUA Press Release.

Source: NCUA

2019 Terrorist Assets Report

OFAC has released the 2019 Terrorist Assets Report. This is the 28th annual report to Congress on assets in the U.S. relating to terrorist countries and organizations engaged in international terrorism.

Source: OFAC

FinCEN Issues COVID-19 Scam Alert

The Financial Crimes Enforcement Network (FinCEN) issued Notice FIN-2020-NTC4 yesterday to alert financial institutions about the potential for fraud, ransomware attacks, or similar types of criminal activity related to COVID-19 vaccines and their distribution. The notice also provides specific instructions for filing Suspicious Activity Reports (SARs) regarding such suspicious activity related to COVID-19 vaccines and their distribution.

Source: FinCEN

OFAC Adds FAQs On Chinese Military Companies

OFAC has posted a Notice of Recent Actions to announce new Frequently Asked Questions related to Executive Order 13959, "Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies," issued on November 12, 2020. OFAC also published a list of entities identified in or in accordance with E.O. 13959 as Communist Chinese military companies, with identifying information.

Source: OFAC

NCUA Board Approves Rules and Proposals

The National Credit Union Administration Board held the first of two consecutive open meetings in December. At the meeting, the Board approved these five items:

- A final rule on subordinated debt.
- A temporary final rule that extends regulatory relief measures in response to COVID-19.
- A proposed rule that permits federal credit unions to purchase mortgage-servicing rights from other federal credit unions under certain conditions.
- A proposed rule revising the definition of a service facility for multiple common bond federal credit unions; and
- A proposed rule on overdraft policy

Source: NCUA

FATF Updates COVID-19 Report

The FATF issued a report in May 2020 highlighting COVID-19-related money laundering and terrorist financing risks and policy responses. Last month it released an update to the report, highlighting the latest developments.

Using input from the FATF Global Network of over 200 countries and jurisdictions, and from private and public sector webinars in July and September, the update details how criminals continue to exploit the crisis. A selection of case studies illustrates how the risks have evolved as the pandemic has progressed, and how authorities have dealt with them. These include mounting cases of counterfeiting medical goods, cybercrime, investment fraud, charity fraud and abuse of economic stimulus measures.

To respond to evolving risks, FATF urged authorities and the private sector to take a risk-based approach, as required by the FATF Standards. This means mitigating the money laundering and terrorist financing risks without disrupting essential and legitimate financial services or driving financial activities towards unregulated service providers.

Source: FATF

FinCEN Proposes Virtual Currency and Digital Assets Rules

The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a proposed rule that would require banks and money services businesses (MSBs) to submit reports, keep records, and verify the identity of customers in relation to transactions above certain thresholds involving CVC/LTDA wallets not hosted by a financial institution (also known as “unhosted wallets”) or CVC/LTDA wallets hosted by a financial institution in certain jurisdictions identified by FinCEN.

The proposed rule complements existing BSA requirements applicable to banks and MSBs by proposing to add reporting requirements for CVC and LTDA transactions exceeding $10,000 in value. Pursuant to the proposed rule, banks and MSBs will have 15 days from the date on which a reportable transaction occurs to file a report with FinCEN. Further, the proposed rule would require banks and MSBs to keep records of a customer’s CVC or LTDA transactions and counterparties, including verifying the identity of their customers, if a counterparty uses an unhosted or otherwise covered wallet and the transaction is greater than $3,000.

The comment period for this new rule expired on 1/4/2021, so stay tuned for an update should it be enacted.

Source: FinCEN

Solar Winds - What to do Next?

The network management software firm SolarWinds experienced a massive cyberattack in March that went undetected until mid-December. The breach pushed malicious code to an estimated 18,000 SolarWinds customers via an update of the company's Orion software. These customers included government agencies, Fortune 500 companies, financial institutions, and vendors serving financial institutions.

Many credit unions are currently in the process of determining what, if any, impact this breach will have on their IT operations:

- Credit unions running SolarWinds Orion software should refer to the company's security alert(s) to determine whether systems were compromised, and obtain the company's breach mitigation recommendations.
- Non-SolarWinds customers aren't necessarily in the clear. They'll need to contact their IT vendors to determine whether they utilized the SolarWinds Orion software, and if so, what steps they're talking to ensure that the credit union's data is secure.
- Affected credit unions should contact their cyber-liability insurance provider to help manage this process and determine next steps, as appropriate.

What if credit union member data was compromised? The credit union will need to follow its incident response program per Part 748, Appendix B of NCUA's regulations if there has been unauthorized access to sensitive member information retained in "member information systems" (i.e., "all of the methods used to access, collect, store, use, transmit, protect, or dispose of member information," including systems maintained by the credit union's service providers).

The credit union's data breach response program should contain procedures to:

- Assess the nature and scope of an incident; identify what member information systems and types of member information have been accessed or misused.
- Notify the appropriate NCUA Regional Director or applicable state supervisory authority as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of "sensitive" member information.
- Notify appropriate law enforcement authorities in situations involving criminal violations requiring immediate attention.
- File a timely Suspicious Activity Report (SAR) for reportable violations.
- Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information (e.g., monitoring, freezing, or closing affected accounts) while preserving records and other evidence.
- Notify affected members when the incident involves unauthorized access to member information systems that could result in substantial harm or inconvenience to the member.

Lastly, don't forget about state law! Please check with your state league regarding state data breach requirements.

Source: CUNA Compliance Blog

Articles of Interest

- CUs and Members Benefit from New PPP Round

- Mortgage Servicer Settles with CFPB
- CFPB Announces Second Piece of FDCPA Final Rule
- Don’t Just Respond to Consumer Expectations – Lead Them
- CU Trades: Economic Impact Payments Will Cause Headaches at Credit Unions
- State Leagues, Others Donate Millions for Pandemic Relief Efforts

CUNA's Advocacy Resources:

- Happenings in Washington

WOCCU Advocacy Resources:

- Telegraph
- Advocate Blog

Compliance Calendar

- January 18th, 2021: Birthday of Martin Luther King, Jr. - Federal Holiday
- January 31st, 2021: **5300 Call Report Due to NCUA**
- February 15th, 2021: President's Day - Federal Holiday
- March 1st, 2021**: Mandatory Use of Updated the Uniform Residential Loan Application (URLA)**
- March 19th, 2021: **Expanding Same Day ACH Effective Date (Date Extended)**