Regulatory Dispatch

Timely news and resources community bankers can use

to better stay on top of a rapidly changing world.

Executive Order on Ensuring Responsible Development of Digital Assets

Section 1. Policy. Advances in digital and distributed ledger technology for financial services have led to dramatic growth in markets for digital assets, with profound implications for the protection of consumers, investors, and businesses, including data privacy and security; financial stability and systemic risk; crime; national security; the ability to exercise human rights; financial inclusion and equity; and energy demand and climate change. In November 2021, non-state issued digital assets reached a combined market capitalization of $3 trillion, up from approximately $14 billion in early November 2016. Monetary authorities globally are also exploring, and in some cases introducing, central bank digital currencies (CBDCs).

While many activities involving digital assets are within the scope of existing domestic laws and regulations, an area where the United States has been a global leader, growing development and adoption of digital assets and related innovations, as well as inconsistent controls to defend against certain key risks, necessitate an evolution and alignment of the United States Government approach to digital assets. The United States has an interest in responsible financial innovation, expanding access to safe and affordable financial services, and reducing the cost of domestic and cross-border funds transfers and payments, including through the continued modernization of public payment systems. We must take strong steps to reduce the risks that digital assets could pose to consumers, investors, and business protections; financial stability and financial system integrity; combating and preventing crime and illicit finance; national security; the ability to exercise human rights; financial inclusion and equity; and climate change and pollution.

Comment: This EO clearly contemplates the creation of an extensive regulatory framework for these assets, including appropriate consideration of their potential for fiscal mischief.

Community Banker Q&A

Q: We have a loan application on which the property address we were given was wrong. For example, we were given the address of 1501 Elm Street but the correct address is 1510 Elm Street. If we disclosed 1501 Elm Street on our LE, can this be corrected on the CLoD or do we need to issue a revised LE?

A: It is a clerical mistake – but it could be a problem. Generally speaking, a revised LE is required when you have both a valid changed circumstance and a tolerance issue you wish to reset. But an error in the property address can't always be corrected under the "clerical error" exception if it would have affected the delivery of the disclosures.

…snip

1. Requirements. Section 1026.19(f)(2)(iv) requires the creditor to deliver or place in the mail corrected disclosures if the disclosures provided pursuant to § 1026.19(f)(1)(i) contain non-numeric clerical errors. An error is considered clerical if it does not affect a numerical disclosure and does not affect requirements imposed by § 1026.19(e) or (f). For example, if the disclosure identifies the incorrect settlement service provider as the recipient of a payment, then § 1026.19(f)(2)(iv) requires the creditor to deliver or place in the mail corrected disclosures reflecting the corrected non-numeric disclosure no later than 60 days after consummation. However, if, for example, the disclosure lists the wrong property address, which affects the delivery requirement imposed by § 1026.19(e) or (f), the error would not be considered clerical.

Source link.

Based on the fact that you used the best information available at the time the LE was issued (assuming the borrower was the best source of the information), correcting the address on CloD with the actual property address is appropriate.

You will need to be able to document that having the wrong property address did not affect your ability to timely deliver disclosures to the applicant.

Items of Interest

Bank Management

	CSBS What's Causing Inflation? What's the Impact? (03/09/2022) - "States of the Economy" is a monthly look at the economic picture across the country. In this episode CSBS Senior Economist Tom Siems and host Matt Longacre discuss what the latest inflation and jobs numbers, business confidence measures and more are telling us about the current trajectory of the U.S. economy. ***Comment: Supply chain issues, surging demand, production costs, and swaths of relief funds all have a role to play, but economists tend to point the finger at the supply chain or the $1.9 trillion American Rescue Plan Act of 2021 as the main culprits.***
	OCC Acting Comptroller Discusses Climate Risk Management, Diversity and Inclusion (03/07/2022) - WASHINGTON—Acting Comptroller of the Currency Michael J. Hsu today discussed climate-related financial risk and the importance of promoting diversity and inclusion in the banking industry at the Institute of International Bankers Annual Washington Conference. Remarks (PDF) Acting Comptroller of the Currency Michael J. Hsu ***Comment: At least for now, the Comptroller is clearly directing expectations on these areas at the largest banks. In December 2021, the OCC released 'Draft Principles for Climate Risk Management' for banks with more than $100 billion in total assets. Nonetheless, all banks must begin their planning to address these areas.***

FDIC Consumer News - March 2022 (03/07/2022) - A path toward building financial stability

The idea of economic inclusion is providing opportunities to access safe and affordable insured bank accounts to all individuals, and paving the way to save, build assets, and maintain financial stability. Effective financial education helps people gain the skills and confidence necessary to sustain a banking relationship, achieve financial goals, and improve financial well-being. An account relationship is fundamental to participation in the banking system. With a banking relationship, consumers can build savings and create a path to obtain credit to meet their goals, such as owning a home or starting a business. No matter where you are on your path to financial stability, the FDIC provides ways to support your financial progress.

Comment: This issue really promotes the notion that developing a relationship with an insured bank is a step on the way to financial success. Consider using these materials in your CRA financial literacy outreach.

BSA / AML

FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts (03/07/2022) - WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today issued a FinCEN Alert, advising all financial institutions to be vigilant against potential efforts to evade the expansive sanctions and other U.S.-imposed restrictions implemented in connection with the Russian Federation's further invasion of Ukraine. The alert provides examples of red flags to assist in identifying suspected sanctions evasion activity and reminds financial institutions of their reporting obligations under the Bank Secrecy Act.

"In the face of mounting economic pressure on Russia, it is vitally important for U.S. financial institutions to be vigilant about potential Russian sanctions evasion, including by both state actors and oligarchs," said Acting Director Him Das. "Although we have not seen widespread evasion of our sanctions using methods such as cryptocurrency, prompt reporting of suspicious activity contributes to our national security and our efforts to support Ukraine and its people."

In recent days [and weeks], the United States and its key partners and global allies have imposed unprecedented economic pressure on Russia and Belarus. As a result, sanctions evasion may occur through various means, including through currently unsanctioned Russian and Belarusian banks or other financial institutions that retain at least some access to the international financial system.

While large scale sanctions evasion using convertible virtual currency (CVC) by a government such as the Russian Federation is not necessarily practicable, CVC exchangers and administrators and other financial institutions may observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian, and other affiliated persons. In addition, FinCEN reminds financial institutions of the dangers posed by Russian-related ransomware campaigns.

All financial institutions—including those with visibility into cryptocurrency or CVC flows, such as CVC exchangers and administrators—should identify and report suspicious activity associated with potential sanctions evasion quickly and conduct appropriate, risk-based customer due diligence or enhanced due diligence where required. Financial institutions are also encouraged to make full use of the information sharing authorities provided by Section 314(b) of the USA PATRIOT Act.

Relevant information to assist with law enforcement investigations will be shared with the U.S. Department of Justice, international partners, and task forces that are established to track and freeze the assets of Russian elites.

Comment: Not only the BSA Department but also operations and new accounts should be familiar with these campaigns and be prepared to identify and report. The alert also warned of possible ransomware attacks.

Deposit / Retail Operations

FTC Fraud and Older Adults – What's Your Story? (03/10/2022) - Every year millions of people report fraud, scams, and bad business practices to the FTC. Your stories help us better understand how fraud affects every community. During National Consumer Protection Week, we're offering information and advice for some of these communities, and today we're focusing on scams that have an impact on older adults.

- Scammers are using social media for investment, romance, and online shopping scams. More than one in four people who reported losing money to fraud from 2020 - 2021 said it started on social media with an ad, a post, or a message. The most money was lost to investment and romance scams.

- Romance scammers pursue people on dating apps and social media with fake tales of love, then demand payments with gift cards, wire transfers, and cryptocurrency. The median reported loss across all romance scam reports was $2,400 last year, but the amount was higher among older adults. People 70 and over reported the highest median losses at $9,000.

- Imposters posing as Amazon workers tricked people with messages about suspicious activity or unauthorized purchases on their accounts. Among people age 60 and over who reported the calls in 2020-2021, the median reported loss was $1,500, compared to $814 for people under age 60.
-

If you spot one of these — or another — scam, please tell us at ReportFraud.ftc.gov. It's easy to report and the information you give helps protect your community. Want more consumer protection news? Read common scams and sign up for email updates.

Comment: National Consumer Protection Week has concluded, but the excellent material provided by the FTC is always helpful in educating consumers—and bank employees—

about common scams. And, don't forget the importance of elder financial abuse training.

Lending

FRB Consumer Credit G.19 (03.07.2022) - Beginning with the April 2022 G.19 Consumer Credit release, scheduled to be published on June 7, 2022, the release will no longer report the Commercial Bank Interest Rates for 48-month New Car Loans. Instead, the release will report the Commercial Bank Interest Rates for 72-month New Car Loans. For more information, please see the announcement posted on March 7, 2022.

January 2022

In January, consumer credit increased at a seasonally adjusted annual rate of 1.9 percent. Revolving credit decreased at an annual rate of 0.3 percent, while nonrevolving credit increased at an annual rate of 2.5 percent.

Technology / Security

CISA Statement From Director Easterly On The Passage Of Cyber Incident Reporting Legislation (03/11/2022) - WASHINGTON – Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly released the following statement today:

"As the nation's cyber defense agency, CISA applauds the passage of cyber incident reporting legislation. Thanks to the support of our many partners in Congress, CISA will have the data and visibility we need to help better protect critical infrastructure and businesses across the country from the devastating effects of cyber-attacks.

"CISA will use these reports from our private sector partners to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure. This information will fill critical information gaps and allow us to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims. CISA is committed to working collaboratively and transparently with our industry and federal government partners in order to enhance the security and resilience of our nation's networks and critical infrastructure.

"Put plainly, this legislation is a game-changer. Today marks a critical step forward in the collective cybersecurity of our nation.

"We are also grateful to Congress for the unprcedented level of funding provided for CISA in the Fiscal Year 2022 Omnibus. This investment represents a recognition of the importance of our mission and the confidence of the Congress in our ability to defend our nation's networks and critical infrastructure."

	Comment: This bill was a bipartisan effort—demonstrating the concern that Congress has regarding reporting. Now we wait and see what kind of regulations are developed to flesh out the requirements. Remember that this is in addition to the computer-security incident rule adopted November 2021.

Selected federal rules – proposed

Proposed rules are included only when community banks may want to comment. Date posted may not be the same as the Federal Register Date.

PROPOSED RULE WITH REQUEST FOR PUBLIC COMMENT

01.26.2022 Request for Information Regarding Fees Imposed by Providers of Consumer Financial Products or Services - The Consumer Financial Protection Bureau (Bureau or CFPB) is seeking comments from the public related to fees that are not subject to competitive processes that ensure fair pricing. The submissions to this request for information will serve to assist the CFPB and policymakers in exercising its enforcement, supervision, regulatory, and other authorities to create fairer, more transparent, and competitive consumer financial markets. **DATES: Comments must be received on or before March 31, 2022.**

01.25.2022 Pilot Program on Sharing of Suspicious Activity Reports and Related Information With Foreign Branches, Subsidiaries, and Affiliates - FinCEN is issuing this notice of proposed rulemaking to seek public comment on the proposed establishment of a limited-duration pilot program, subject to conditions set by FinCEN, to permit a financial institution with a suspicious activity report (SAR) reporting obligation to share SARs and information related to SARs with the institution's foreign branches, subsidiaries, and affiliates for the purpose of combating illicit finance risk, in accordance with Section 6212(a) of the Anti-Money Laundering Act of 2020 (AML Act). **DATES: Written comments on this proposed rule must be received on or before March 28, 2022.**