



# Community Bankers of Michigan Regulatory Dispatch

April 6, 2022

*Timely news and resources community bankers can use*

*to better stay on top of a rapidly changing world.*

## **FDIC Consumer Compliance Supervisory Highlights**

Consumer Compliance Supervisory Highlights is published by the FDIC's Division of Depositor and Consumer Protection to provide an overview of consumer compliance issues identified through the FDIC's supervision of state non-member banks and thrifts in 2021.

This [Spring 2022 - PDF issue](#) includes:

- A description of the most frequently cited violations and other consumer compliance examination observations.
- Information on regulatory developments.
- A summary of consumer compliance resources and information available to financial institutions; and
- An overview of consumer complaint trends.

***Comment: Perhaps it is no surprise, but TILA violations are 40% of total violations. Of particular interest, the FDIC also describes several fair lending cases referred to the DOJ in 2020. In the examples provided, the FDIC concluded there was sufficient evidence to conclude the bank had engaged in a 'practice of discrimination.'***

## **CBM Insights**

Q: When doing some account reviews, we noticed information on an existing customer that needed updating. We ran that customer thru a new account platform we recently started using. Her SS number came up to deceased person. A CTR had already been filed. Should this be amended? The customer is supposed to be providing us with an ITIN.

A: You have two issues here. The first is filing a SAR for potential identity theft, and the second is filing corrected CTR(s).

FinCEN has made it clear which errors must be corrected and which ones do not require correction; based on either a Primary or Secondary error type. But that really addresses CTR batch files and not individual errors identified by the bank.

*Attachment B – Error Correction Instructions*

*This attachment identifies the requirements and procedures for correcting FinCEN CTR errors reported to batch filers during the FinCEN CTR acknowledgement process.*

## Error Categories:

There are two types of errors identified in batch files: format errors that may result in automatic rejection of a batch file and file errors that represent errors in data entered in individual fields. Format errors prevent the batch file from being processed. For example, error F18 “A required 9Z record is missing from the submitted file” is a fatal format error because each batch file must contain a 9Z record. Error C404 “Person street address is blank” is a file error because it indicates data is missing from a street address field. A batch file with large numbers of file errors can be rejected by the BSA E-Filing Program if the number of errors exceeds programming limits.

File errors are classified as primary or secondary errors, depending on their importance. Primary errors are file errors that violate electronic filing requirements or report instructions and so degrade FinCEN CTR data quality that they must be corrected. Primary errors make it difficult for regulators, analysts, and law enforcement investigators to locate the FinCEN CTRs in the database or identify the nature and circumstances of the currency transactions. Examples of such errors include blank last names or legal names, missing financial institution Employer Identification Numbers, or invalid entries in the transaction date field. Attachment A – Error Code List identifies primary errors by adding an asterisk (\*) to the four-digit error code.

Secondary errors are file errors that violate electronic filing requirements or report instructions but have a lesser impact on FinCEN CTR data quality. Examples of secondary errors are ZIP Codes that end in four zeros (e.g. 123450000), blank or invalid financial institution address information, or invalid telephone numbers.

## Correction Requirements:

Filers should immediately correct and resubmit a batch file rejected for fatal format errors or for large numbers of file errors when notified by FinCEN the batch file was not accepted. Rejection of a batch file does not relieve the filer of the responsibility to file a FinCEN CTR within 15 days following the day on which the reportable transaction occurred.

When an accepted batch file contains FinCEN CTRs with primary errors, those FinCEN CTRs must be re-filed as corrected reports with the primary errors corrected.

If the accepted batch file contains FinCEN CTRs with both primary and secondary errors, they must be re-filed as corrected reports with all errors corrected.

FinCEN CTRs that contain only secondary errors need not be re-filed.

Source [link](#). [Page 45]

The general rule is simple. Any error identified by a bank on a CTR that has already been filed should be corrected within 30 days of noting the error.

## Items of Interest

### BSA / AML

**IRS Reminds Holders of Foreign Bank and Financial Accounts of April FBAR Deadline (03/31/2022)** - WASHINGTON – The Internal Revenue Service reminded U.S. citizens, resident aliens and any domestic legal entity that the deadline to file their annual [Report of Foreign Bank and Financial Accounts](#) (FBAR) is April 15. For additional information about filing deadlines, filers should look to [Financial Crimes Enforcement Network’s \(FinCEN\) website](#) for further information.

Filers missing the April deadlines will receive an automatic extension until Oct. 15, 2022, to file the FBAR. They don't need to request the extension. See [FinCEN's website](#) for further information.

The Bank Secrecy Act requires U.S. persons to file an [FBAR](#) if they have:

1. Financial interest in, signature authority or other authority over one or more accounts, such as a bank account, brokerage account, mutual fund or other financial account in a foreign country, and
2. The aggregate value of all foreign financial accounts exceeds \$10,000 at any time during the calendar year.

Because of this threshold, the IRS encourages U.S. persons or entities with foreign accounts, even relatively small ones, to check if this filing requirement applies to them.

A U.S. person is a citizen or resident of the United States or any domestic legal entity such as a partnership, corporation, limited liability company, estate or trust.

***Comment: This applies to certain individuals who have signature authority over, but no financial interest in, one or more foreign (i.e., non-US) financial accounts.***

**FinCEN [2021 SAR Filing Trend Data Now Available on FinCEN's Website](#) (03/28/28)** - The Financial Crimes Enforcement Network's (FinCEN) Interactive SAR Stats webpage now includes Filing Trend Data by industry updated through the 2021 calendar year. The new downloadable data is arranged by industry type and includes rankings by states/territories and suspicious activities. It is available at <https://www.fincen.gov/reports/sar-stats/sar-filings-industry>.

Interactive SAR Stats is an application that enables users to view FinCEN's trend data for aggregated counts of defined suspicious activities that financial institutions file with FinCEN as required by the Bank Secrecy Act.

This announcement underscores FinCEN's commitment to safeguarding the financial system from illicit use, combatting money laundering, and promoting national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

***Comment: The reports include interesting breakdowns on types of SAR filings, among other data.***

## Deposit / Retail Operations

No news to report this week.

## Human Resources

No news to report this week.

## Lending

	<p><b>FFIEC <a href="#">Issues 2022 Edition of the Guide to HMDA Reporting: Getting It Right!</a></b> (04/01/2022) - The 2022 edition of the "Guide to HMDA Reporting: Getting It Right!" is now available at <a href="http://www.ffiec.gov/hmda/guide.htm">www.ffiec.gov/hmda/guide.htm</a>.</p> <p>The 2022 version was developed by member agencies of the Federal Financial Institutions Examination Council and includes appendices that provide additional implementation materials you may find useful.</p> <p><b><i>Comment: The Guide is a valuable resource for assisting all banks in their HMDA reporting. It includes a summary of responsibilities and requirements, directions for assembling the necessary tools, and instructions for reporting HMDA data.</i></b></p>
	<p><b>OCC <a href="#">Commercial Real Estate Lending: Revised Comptroller's Handbook Booklet and Rescissions</a></b> (03/29/2022) - The Office of the Comptroller of the Currency (OCC) issued version 2.0 of the "Commercial Real Estate Lending" booklet of the Comptroller's Handbook. This booklet discusses risks and risk management practices associated with commercial real estate. This booklet also provides examiners with a framework for evaluating commercial real estate lending activities.</p> <p><b>Rescissions</b> The updated booklet replaces version 1.1 of the booklet of the same title issued in January 2017. Also rescinded is OCC Bulletin 2013-19, "Commercial Real Estate Lending: Comptroller's Handbook Revisions and Rescissions," which transmitted version 1.0 of the booklet of the same title issued in August 2013.</p> <p><b>Note for Community Banks</b> The "Commercial Real Estate Lending" booklet applies to the OCC's supervision of community banks<sup>1</sup> engaged in commercial real estate lending.</p> <p><b>Highlights</b> The updated booklet</p> <ul style="list-style-type: none"><li>• reflects changes to laws and regulations since this booklet was last updated.</li><li>• reflects OCC issuances published and rescinded since this booklet was last updated.</li><li>• includes clarifying edits regarding supervisory guidance, sound risk management practices, and legal language.</li><li>• revises certain content for general clarity.</li></ul> <p><b>Related Link</b> <a href="#">"Commercial Real Estate Lending"</a></p> <p><b><i>Comment: Don't overlook the pandemic's impact on commercial rental properties as more and more businesses continue to permit or require remote working.</i></b></p>

## Technology / Security

	<p><b>CISA <a href="#">Readout from Second Cybersecurity Advisory Committee Meeting</a></b> (03/31/2022) - WASHINGTON - The Cybersecurity and Infrastructure Security Agency (CISA) held its second Cybersecurity Advisory Committee meeting. The Committee, which held its inaugural meeting in December 2021, includes a diverse slate of leaders from across</p>
--	---

industry, academia, and government. Through their unique insight, the Committee members will ultimately provide recommendations on the development and refinement of CISA's cybersecurity programs and policies. During the meeting, subcommittee chairs provided Director Jen Easterly with an update on the progress being made on key objectives outlined by the Director during the Committee's inaugural meeting.

The next Cybersecurity Advisory Committee will be held in-person on June 22, 2022 in Austin, Texas. Details and information on how to attend will be forthcoming.

**FDIC [Computer-Security Incident Notification Implementation](#) (03/29/2022)** - On November 23, 2021, the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency (collectively, the agencies) issued a joint final rule to establish computer-security incident notification requirements (Final Rule) for banking organizations and their bank service providers. Banks and their service providers must comply with the Final Rule starting May 1, 2022.

FDIC-supervised banks can comply with the rule by reporting an incident to their case manager, who serves as the primary FDIC contact for all supervisory-related matters, or to any member of an FDIC examination team if the event occurs during an examination. If a bank is unable to access its supervisory team contacts, the bank may notify the FDIC by email at: [incident@fdic.gov](mailto:incident@fdic.gov).

Bank service providers must notify any affected FDIC-supervised banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, services provided to such banking organization for four or more hours.

A copy of the [Final Rule](#) is available on the FDIC's website.

Statement of Applicability: The contents of, and material referenced in, this FIL apply to all FDIC-insured financial institutions

Highlights:

- FDIC-supervised banks can comply with the rule by notifying their case manager of an incident.
- FDIC-supervised banks can comply with the rule by notifying any member of an FDIC examination team if the event occurs during an examination.
- If a bank is unable to access its supervisory team contacts, the bank may notify the FDIC by email at: [incident@fdic.gov](mailto:incident@fdic.gov).

[Computer-Security Incident Notification Final Rule](#)

***Comment: In December 2021, the prudential regulators issued a final rule that requires a banking organization to notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident," as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. The agencies have provided an effective date of April 1, 2022, and a compliance date of May 1, 2022.***

**OCC Information Technology: [OCC Points of Contact for Banks' Computer-Security Incident](#)**

**[Notifications](#)** (03/29/2022) - Effective May 1, 2022, banks must use the designated points of contact listed in this bulletin to satisfy the incident notification requirements established in the interagency final rule for banks and their bank service providers dated November 23, 2021. The Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation published the final rule to help promote early awareness of emerging threats to banks, their bank service providers, and the broader financial system and to help the agencies react to these threats before they become systemic.

Banks and their bank service providers must comply with the final rule starting May 1, 2022. Under the final rule, a notification incident generally includes a significant computer-security incident that disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability of the bank's operations; results in customers being unable to access their deposit and other accounts; or impacts the stability of the financial sector. Incidents may include a major computer-system failure; a cyber-related interruption, such as a distributed denial of service or ransomware attack; or another type of significant operational interruption.

Note for Community Banks: This bulletin applies to community banks.

**Highlights:**

- A bank must notify the OCC after the bank determines that a notification incident has occurred, and the OCC must receive this notice as soon as possible and no later than 36 hours after the bank's determination.
- To satisfy the notification requirement, the bank may email or call its supervisory office, submit a notification via the BankNet website, or contact the BankNet Help Desk starting on May 1, 2022. Refer to the "OCC Points of Contact for Banks" section of this bulletin.

**OCC Points of Contact for Banks:**

Starting on May 1, 2022, banks may satisfy the notification requirement of the final rule by contacting their supervisory office or by using one of the following to communicate a notification incident:

- BankNet
  - Registered BankNet members may securely submit an incident from the home page. The OCC recommends that users [register for BankNet](#) well before an incident occurs.
- BankNet Help Desk
  - Email: [BankNet@occ.treas.gov](mailto:BankNet@occ.treas.gov)
  - Phone: (800) 641-5925

If a bank is unsure whether it is experiencing a notification incident for purposes of the final rule, the bank should contact its supervisory office.

**Related Links**

[BankNet](#)

[OCC Bulletin 2021-55](#), "Computer-Security Incident Notification: Final Rule"

*Comment: While very similar to the FDIC incident notification, this one is for national banks.*

## 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**

**03.25.2022** [FDIC Request for Information on Bank Merger Act](#) - The Federal Deposit Insurance Corporation sent for publication in the Federal Register a Request for Information (RFI) seeking information and comments regarding the application of the laws, practices, rules, regulations, guidance, and statements of policy (together, regulatory framework) that apply to merger transactions involving one or more insured depository institution, including the merger between an insured depository institution and a noninsured institution. **Dates: Comments are due within 60 days of publication in the Federal Register.**

**03.22.2021** [Rules to Enhance and Standardize Climate-Related Disclosures for Investors](#) - The Securities and Exchange Commission today proposed rule changes that would require registrants to include certain climate-related disclosures in their registration statements and periodic reports, including information about climate-related risks that are reasonably likely to have a material impact on their business, results of operations, or financial condition, and certain climate-related financial statement metrics in a note to their audited financial statements. The required information about climate-related risks also would include disclosure of a registrant's greenhouse gas emissions, which have become a commonly used metric to assess a registrant's exposure to such risks. The proposing release will be published on SEC.gov and in the Federal Register. **The comment period will remain open for 30 days after publication in the Federal Register, or 60 days after the date of issuance and publication on sec.gov, whichever period is longer.**

**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: On March 25, the CFPB [extended the comment period](#) until April 11, 2022.**