FDIC Advisory Committee on Community Banking

May 3, 2022

Supervision and Policy Update

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

FDIC Advisory Committee on Community Banking

May 3, 2022

Crypto-Related Activities

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Notification of Engaging in Crypto-Related Activities FIL-16-2022

Background

- Addresses the engagement by FDIC-supervised institutions in crypto-related activities
- Crypto-related activities may pose significant safety and soundness risks, as well as financial stability and consumer protection concerns
- Risks and concerns are evolving as these activities are not yet fully understood
    - Little consistency in definitions (difficult to categorically identify crypto-assets and crypto-related activities)
    - Structure/scope of activities is rapidly changing/expanding
    - Difficult to adequately assess risks without considering each crypto-related activity individually

FDIC

Notification of Engaging in Crypto-Related Activities FIL-16-2022

Scope

- Applies to all FDIC-supervised institutions
  - Notify the FDIC of any current or planned crypto-related activities
  - Provide all necessary information that would allow the FDIC to engage with the institution regarding related risks*
- Legal implications include the safety and soundness standards set forth in Appendices A and B of Part 364 of the FDIC Rules and Regulations

* The FDIC will provide supervisory feedback as appropriate

FDIC

Notification of Engaging in Crypto-Related Activities FIL-16-2022

Risk Considerations – Safety & Soundness

- Fundamental ownership issues
- Anti-money laundering/countering the financing of terrorism implications
- Information technology and information security implications
- Credit risk exposure posed by the crypto asset or the structure of the asset; counterparty risk
- Market and liquidity risk

FDIC

Notification of Engaging in Crypto-Related Activities FIL-16-2022

Risk Considerations – Financial Stability

- Systemic risks may arise as an unintended consequence of interconnected structures (e.g., runs, contagion, asset fire sales)
- Operational failures may have a destabilizing effect on insured depository institutions

FDIC

Notification of Engaging in Crypto-Related Activities FIL-16-2022

Risk Considerations – Consumer Protection

- Risk of consumer confusion regarding crypto assets offered by, through, or in connection with insured depository institutions, as consumers may not understand the role of the bank or the speculative nature of certain crypto assets as compared to traditional banking products
- Effective management of the application of consumer protection requirements to new and changing crypto-related activities

FDIC

Notification of Engaging in Crypto-Related Activities FIL-16-2022

Resources

- Notification of Engaging in Crypto-Related Activities FIL-16-2022
- Standards for Safety and Soundness, Section 39 of the Federal Deposit Insurance Act 12 U.S.C. 1831p--1(a), 12 CFR Part 364

FDIC

FDIC Advisory Committee on Community Banking

May 3, 2022

Climate Change

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

FDIC Advisory Committee on Community Banking

May 3, 2022

Cybersecurity

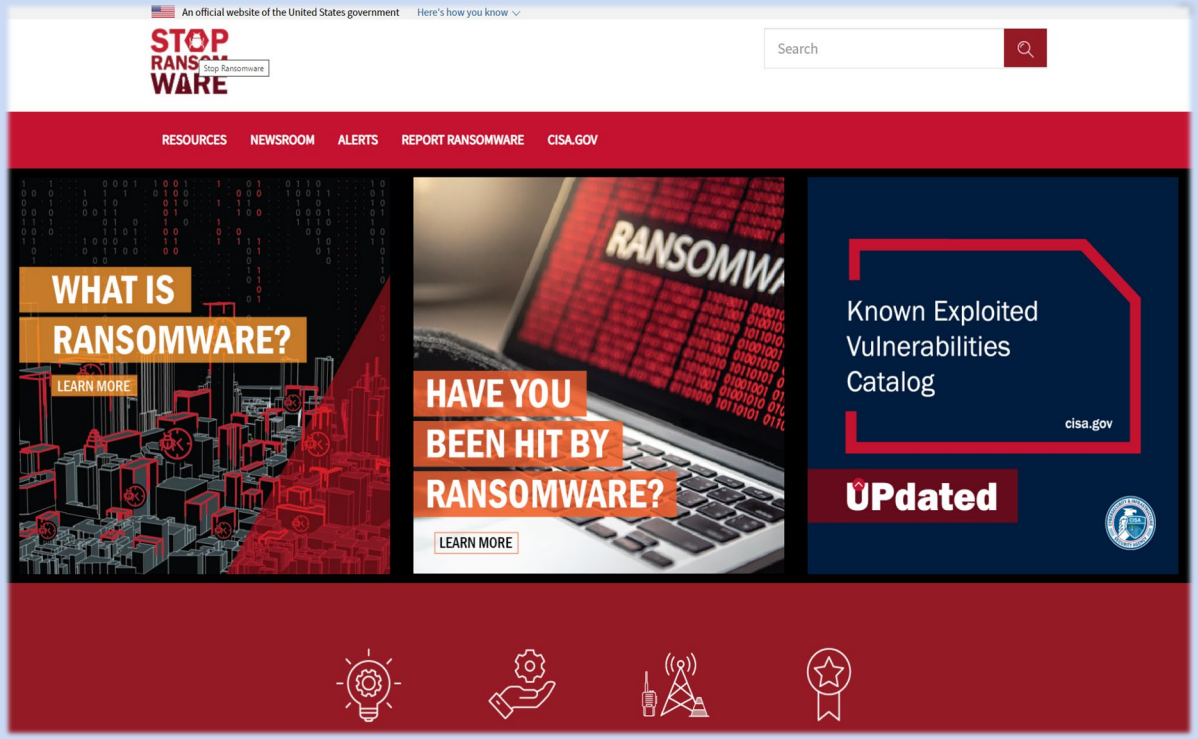
FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Threats

Geo-political

[CISA Shields-Up]

Ransomware



[CISA Stop Ransomware]

FDIC

Incident Notification

FDIC Notification Rule

Home // News // Financial Institution Letters // 2021

Financial Institution Letter

Computer-Security Incident Notification Final Rule

November 18, 2021 | FIL-74-2021 Share This:

Contact:

supervision@fdic.gov

Notes:

Access FDIC Financial Institution Letters (FILs) on the FDIC's website.

Subscribe to receive FILs electronically.

About the FDIC:

The Federal Deposit Insurance Corporation (FDIC) is an independent

Summary:

The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Board), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) have issued a joint final rule to establish computer-security incident notification requirements for banking organizations and their bank service providers.

The rule will provide the agencies with early awareness of emerging threats to banking organizations and the broader financial system, including potentially systemic cyber events.

A copy of the Final Rule can be found on the FDIC's website.

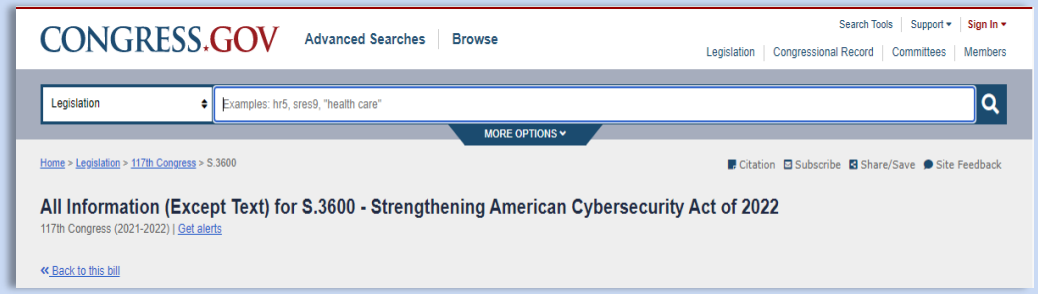
Statement of Applicability: This Financial Institution Letter (FIL) applies to all FDIC-supervised institutions.

Highlights:

- FDIC-supervised banking organizations will be required to notify the FDIC as soon as possible and no later than 36 hours after the banking organization determines that a computer-security incident that rises to the level of a notification incident has occurred. The banking organization must provide this notification to the appropriate FDIC supervisory office, or an FDIC-designated point of contact, through email, telephone, or other similar methods that the FDIC may prescribe.
- The rule defines computer-security incident as an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.
- A notification incident is defined as a computer-security incident that has materially disrupted or degraded, or is reasonably

[Financial Institution Letter 74-2021]

Strengthening American Cybersecurity Act of 2022



CONGRESS.GOV Advanced Searches | Browse

Search Tools | Support | Sign In

Legislation | Congressional Record | Committees | Members

Legislation | Examples: hr5, sres9, "health care"

MORE OPTIONS

Home > Legislation > 117th Congress > S.3600

Citation | Subscribe | Share/Save | Site Feedback

All Information (Except Text) for S.3600 - Strengthening American Cybersecurity Act of 2022

117th Congress (2021-2022) | Get alerts

« Back to this bill

FDIC

Ransomware Horizontal Review

Background

- Searched FDIC and other agency databases for ransomware attacks over a two-year period (June 2019-May 2021)
- Searched for only attacks at FDIC-supervised institutions
  - Identified 36 ransomware attacks of interest
- The FDIC reviewed forensic reports from, and conducted interviews with, attacked financial institutions

FDIC

Ransomware Horizontal Review

- The FDIC developed a “Severity Matrix” and examined forensic reports and interview transcripts in depth for control success and failures.
  - **High**: Ransom paid, loss of services, loss of data, lateral movement, persistence
  - **Moderate**: Lateral movement or persistence without loss of data or services
  - **Low**: Attack stopped before significant impact or cost

FDIC

Ransomware Horizontal Review

- Effective controls used

- Network Segmentation
- Operating System Hardening
- Microsoft Office Macros Disabled
- Intrusion Detection System/ Intrusion Prevention System (analysis indicated partially effective)
- Logging

- Controls that would have been effective

  - Internet Address Filtering
  - Backup Isolation
  - Unauthorized Executables Prevention
  - PowerShell Access Prevention
  - Multi-Factor Authentication
  - Excess Permissions Prevention

FDIC

FDIC Advisory Committee on Community Banking

May 3, 2022

Anti-Money Laundering and Sanctions Updates

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Anti-Money Laundering (AML) Updates

Anti-Money Laundering Act of 2020

- AML/Countering the Financing of Terrorism Priorities
- Review regulations implementing the Bank Secrecy Act (BSA)
- Corporate Transparency Act

BSA/AML Examination Manual

- Updates
- Banker webinar on April 12, 2022

Sanctions Updates

- The Office of Foreign Assets Control (OFAC) issued many Russian-related sanctions and general licenses.
  - Russian elites, oligarchs, other individuals, banks, and other entities were added to the Specially Designated Nationals List (SDN List).
  - Assets of individuals and entities on the SDN List should be blocked, while other transactions should be rejected.
  - OFAC issued many general licenses to allow transactions that otherwise would be prohibited.
- The Financial Crimes Enforcement Network issued an advisory, *Increased Vigilance for Potential Russian Sanctions Evasion Attempts*.

FDIC Advisory Committee on Community Banking

May 3, 2022

Current Expected Credit Losses (CECL) Update

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Overview

Incurred Loss Methodology	CECL Methodology
When are losses recognized?	
When an incurred loss is “probable”	Expected losses estimated at origination and updated each reporting date
How much loss is recognized?	
Recognize amount of loss already incurred	Reduce amortized cost basis to net collection expectation
How is the loss amount determined?	
Past events and current conditions	Also include reasonable and supportable future expectations

FDIC

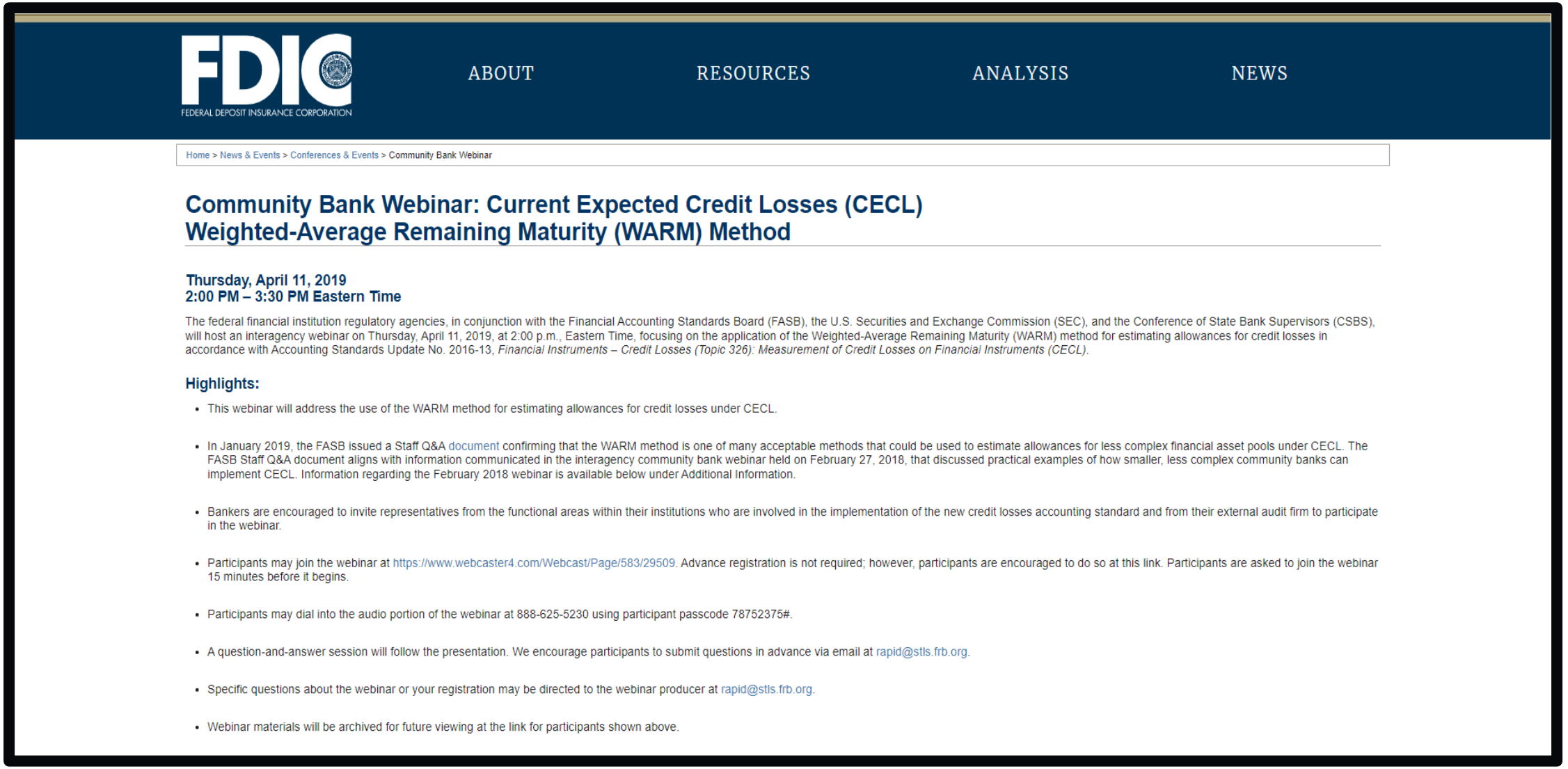
Implementation

Entity	Adoption Date	Call Report Date*
Securities and Exchange Commission filers, excluding entities eligible to be smaller reporting companies (SRCs)	Fiscal years beginning after 12/15/2019, including interim periods within those fiscal years	3/31/2020
All other entities, including SRCs	Fiscal years beginning after 12/15/2022, including interim periods within those fiscal years	3/31/2023
Early application	Early application permitted for fiscal years beginning after 12/15/2018, including interim periods within those fiscal years	Depends

*For entities with calendar year fiscal years

FDIC

CECL Resources



FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

ABOUT RESOURCES ANALYSIS NEWS

Home > News & Events > Conferences & Events > Community Bank Webinar

Community Bank Webinar: Current Expected Credit Losses (CECL) Weighted-Average Remaining Maturity (WARM) Method

Thursday, April 11, 2019
2:00 PM – 3:30 PM Eastern Time

The federal financial institution regulatory agencies, in conjunction with the Financial Accounting Standards Board (FASB), the U.S. Securities and Exchange Commission (SEC), and the Conference of State Bank Supervisors (CSBS), will host an interagency webinar on Thursday, April 11, 2019, at 2:00 p.m., Eastern Time, focusing on the application of the Weighted-Average Remaining Maturity (WARM) method for estimating allowances for credit losses in accordance with Accounting Standards Update No. 2016-13, *Financial Instruments – Credit Losses (Topic 326): Measurement of Credit Losses on Financial Instruments (CECL)*.

Highlights:

- This webinar will address the use of the WARM method for estimating allowances for credit losses under CECL.
- In January 2019, the FASB issued a Staff Q&A document confirming that the WARM method is one of many acceptable methods that could be used to estimate allowances for less complex financial asset pools under CECL. The FASB Staff Q&A document aligns with information communicated in the interagency community bank webinar held on February 27, 2018, that discussed practical examples of how smaller, less complex community banks can implement CECL. Information regarding the February 2018 webinar is available below under Additional Information.
- Bankers are encouraged to invite representatives from the functional areas within their institutions who are involved in the implementation of the new credit losses accounting standard and from their external audit firm to participate in the webinar.
- Participants may join the webinar at https://www.webcaster4.com/Webcast/Page/583/29509. Advance registration is not required; however, participants are encouraged to do so at this link. Participants are asked to join the webinar 15 minutes before it begins.
- Participants may dial into the audio portion of the webinar at 888-625-5230 using participant passcode 78752375#.
- A question-and-answer session will follow the presentation. We encourage participants to submit questions in advance via email at rapid@stls.frb.org.
- Specific questions about the webinar or your registration may be directed to the webinar producer at rapid@stls.frb.org.
- Webinar materials will be archived for future viewing at the link for participants shown above.

FDIC

CECL Resources

- FDIC Resources on CECL
  - Banker Resource Center
    - Supervisory Resources
    - Videos/Webcasts/Teleconferences - WARM Method Webinar
- Interagency Guidance
  - Interagency Policy Statement on Allowances for Credit Losses
  - New Accounting Standard on Credit Losses: Frequently Asked Questions
  - Supervisory Guidance on Model Risk Management
  - Guidance for Managing Third-Party Risk

FDIC

FDIC Advisory Committee on Community Banking

May 3, 2022

Overview of Consumer Compliance Supervisory Highlights

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Consumer Compliance Supervisory HIGHLIGHTS

Federal Deposit Insurance Corporation

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

March 2022

FDIC

Overview

- Each year, the Division of Depositor and Consumer Protection (DCP) issues a Consumer Compliance Supervisory Highlights publication that provides:
  - A summary of FDIC-supervised institutions' overall consumer compliance performance
  - A list of the most frequently cited violations and other consumer compliance examination observations
  - Regulatory and other developments
  - Consumer compliance resources
- This year, we added a new section:
  - An overview of trends in consumer complaints

FDIC

2021 Consumer Compliance Performance, Violations, and Enforcement Actions

- Summary of Overall Consumer Compliance Performance
  - 99% rated Satisfactory or better for consumer compliance as well as for the Community Reinvestment Act (CRA)
- Most Frequently Cited Violations
  - Similar to those cited in 2020
- Enforcement Actions
  - 20 formal and 24 informal actions

FDIC

2021 Consumer Compliance Examination Observations: Electronic Fund Transfers (EFTs)

- The FDIC identified issues involving consumers being targeted for fraud relating to EFTs
- Regulation E's liability protections apply even if a consumer is deceived into giving someone else authorization credentials
- Both a financial institution and a money payment platform have investigative and error resolution obligations

FDIC

2021 Consumer Compliance Examination Observations: Electronic Fund Transfers (EFTs)

- Actions that may mitigate the risks of non-compliance with Regulation E:
  - Reviewing account agreements and disclosures
  - Conducting thorough investigations of fraud-related EFT disputes and documenting the findings
  - Educating consumers about scams and providing tips on avoiding scams
  - Reminding consumers to notify their financial institution if they fall victim to a scam
  - Implementing effective fraud detection and prevention measures
  - Training staff on Regulation E's requirements and assisting consumers alleging unauthorized transactions

FDIC

2021 Consumer Compliance Examination Observations: Overdrafts

- The FDIC identified issues relating to financial institutions converting overdraft programs from a static limit to a dynamic limit
- Institutions did not provide information to customers about the change
- The FDIC cited violations of Section 5 of the Federal Trade Commission (FTC) Act for deceptive acts or practices

2021 Consumer Compliance Examination Observations: Overdrafts

- Actions that may mitigate the risks when implementing automated overdraft programs with dynamic limits:
  - Providing clear and conspicuous information to existing customers
  - Disclosing changes to overdraft limits in real time to customers
  - Reviewing and revising account opening disclosures or other communications used to inform new customers
  - Explaining that the dynamic limit is established based on algorithms, or a set of rules, that weigh numerous variables and customer behaviors, how the limit may change, and how the limit may be suspended or reduced
  - Training customer service and complaint processing staff

FDIC

2021 Consumer Compliance Examination Observations: Re-presentments

- The FDIC identified violations of Section 5 of the FTC Act relating to assessing a non-sufficient funds (NSF) fee when a charge is presented for payment, but cannot be covered by the balance in the account
- The failure to disclose material information to customers about re-presentment practices and fees may be deceptive
- This practice may also be unfair if there is the likelihood of substantial injury to customers

FDIC

2021 Consumer Compliance Examination Observations: Re-presentments

- Actions that may mitigate potential risks of consumer harm and help avoid potential violations of Section 5 of the FTC Act:
  - Eliminating NSF fees
  - Declining to charge more than one NSF fee for the same transaction, regardless of whether the item is re-presented
  - Disclosing the amount of NSF fees and how such fees will be imposed
  - Reviewing customer notification related to NSF transactions and the timing of fees
  - Conducting a comprehensive review of policies, procedures and disclosures
  - Working with service providers to retain comprehensive records so that re-presented items can be identified

FDIC