Community Bankers of Michigan Regulatory Dispatch

September 6, 2023

Timely news and resources community bankers can use

to better stay on top of a rapidly changing world.

FDIC Updates EHL Poster

FDIC-supervised institutions are required to maintain up-to-date Equal Housing Lender (EHL) posters in branches, as required by the Fair Housing Act. The FDIC recently amended some details of the posters, including updating the name of the office to which complaints should be addressed, as well as adding the web address of the FDIC's web-based complaint portal. FDIC-supervised institutions may obtain compliant posters from the FDIC Online Catalog through FDICconnect.

STATEMENT OF APPLICABILITY:
The contents of, and material referenced in, this FIL apply to all FDIC-supervised financial institutions.

DISTRIBUTION:
FDIC-Supervised Financial Institutions

Comment: This goes back to Fall 2022 when the FDIC published a technical correction to the Fair Housing Rule and the Consumer Protection in Sales of Insurance Rule.

CBM Insights

Q. Does the Servicemember Civil Relief Act (SCRA) cover business loans? Does the Military Lending Act (MLA) cover business loans?

A. Let's take MLA first, because it is the easiest - the MLA does not apply to credit that is to be used primarily for a business, commercial, or agricultural purpose. The MLA only applies to 'consumer credit' meaning credit to a 'natural person' and for 'personal, family or household purposes.'

The short answer on the SCRA is that if the service member is personally liable on a debt incurred before entering service, those borrowers are protected.

The long answer is that the text of the SCRA does not distinguish among protections based upon the purpose of a loan. Meaning if a service member is personally liable for repayment of a business or commercial loan, regulators and courts are taking the position that the act covers these loans just as it would any other obligation or debt.

In the court case of Cathey et al. v. First Republic Bank, Stewart and donna Cathey obtained financing to construct a gas station and convenience store. in issuing the loan, the bank required the Catheys to sign all of the promissory notes for these corporate loans "in their individual capacities." Stewart Cathey then entered military service and provided his bank with a copy of his military orders so he could receive the SCRA's interest rate benefit. The bank nevertheless charged him an interest rate that exceeded the SCRA's 6 percent cap. The Catheys sued the bank, and the court held that the bank did not comply with the statute. However, the court made it clear that the loans were eligible for SCRA benefits only because the service member was a signatory: Every single promissory note at issue was signed individually by each plaintiff [including the servicemember] and by the corporation. the notes expressly provide that all three 'promise to pay.' All three are referred to collectively as borrower in the note and in the business loan agreement. Both plaintiffs and the corporation are referred to as borrower in all of the commercial guarantee agreements.

This is not a case where loans were executed by a corporation which happened to be owned in part by a serviceman. Rather, this case involves loans incurred by a serviceman. The fact that the loans were also incurred by others (his wife and his family's corporation) is irrelevant. Thus, the court held the business purpose of the loan was irrelevant so long as the service member was personally obligated on it, the SCRA applied.

Items of Interest

Bank Management

	OCC Hosts Compliance and Operational Risk Workshops in Santa Ana (08/30/2023) - The Office of the Comptroller of the Currency (OCC) will host two workshops in Santa Ana, California, on October 3-4 for directors, senior management, and other key executives of national community banks and federal savings associations. The Compliance Risk: Understanding the Rules workshop on October 3 focuses on the critical elements of an effective compliance risk management program. Participants will review major compliance risks and critical regulations, identify compliance red flags, and learn about common OCC examination findings related to compliance risk. The Operational Risk: Navigating Rapid Changes workshop on October 4 covers key risk management processes, oversight roles and governance responsibilities, fraud, risk-based audit programs, third-party vendor oversight, establishing a strong ethical culture, and regulatory expectations to address cyber threats. The fee for each workshop is $99. Participants receive course materials, supervisory materials, and lunch. To register online and view the schedule and locations of other workshops, visit the OCC's website. For additional questions about the workshops, please contact the OCC Bank Director Workshop Team at (202) 649-6490 or bankdirectorworkshop@occ.treas.gov. ***Comment: Workshops are generally limited to 35 participants. Attendees will receive course materials, supervisory publications and lunch making the programs worth the $99 workshop fee.***

BSA / AML

	No news to report this week.

Deposit / Retail Operations

	FTC Did Someone Insist You Pay Them with Cryptocurrency? (08/28/2023) - What's one of the best ways to spot a scam? Know how scammers tell you to pay. Scammers want you to pay them in ways that are hard to trace and hard to get your money back: like through a gift card, wire transfer, payment app, or cryptocurrency. Here, we'll focus on that last one — cryptocurrency — and how to avoid cryptocurrency-related scams. ***Comment: In early 2023, the federal agencies warned banks that dealing with cryptocurrency exposes them to an array of risks, including scams and fraud.***

Human Resources

	No news to report this week.

Lending

	No news to report this week.

Technology / Security

	CISA and FBI Publish Joint Advisory on QakBot Infrastructure (08/30/2023) - The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA), Identification and Disruption of QakBot Infrastructure, to help organizations detect and protect against newly identified QakBot-related activity and malware. QakBot—also known as Qbot, Quackbot, Pinkslipbot, and TA570—is responsible for thousands of malware infections globally. Originally used as a banking trojan to steal banking credentials for account compromise, QakBot—in most cases—was delivered via phishing campaigns containing malicious attachments or links to download the malware, which would reside in memory once on the victim network. QakBot has since grown to deploy multiple types of malware, trojans, and highly-destructive ransomware variants targeting the United States and other global infrastructures, including the Election Infrastructure Subsector, Financial Services, Emergency Services, and Commercial Facilities Sectors. CISA and FBI urge organizations to implement the recommendations contained within the joint CSA to reduce the likelihood of QakBot-related activity and promote identification of QakBot-facilitated ransomware and malware infections. To report incidents and anomalous activity, please contact one of the following organizations: • CISA, either through the agency's online tool (cisa.gov/report) or the 24/7 Operations Center at report@cisa.gov or (888) 282-0870. • FBI via a local field office. Organizations are also encouraged to visit CISA's Malware, Phishing, and Ransomware and StopRansomware.gov pages—StopRansomware provides a range of free U.S. government resources and services that can help bolster cyber hygiene, cybersecurity posture and reduce risk to ransomware, and contains an updated Joint #StopRansomware Guide. ***Comment: Train. Train. Remind. Remind. Train. The great innovation of QakBot attacks that makes them very difficult to detect is that the person receives an email with a hyperlink. However, this message often compromises benign domains and hosts the malicious payload. In addition, it is designed***

	to appear from people with whom the individual frequently interacts, is even part of a conversation thread, and prompts "click to view attachment." so they trust and click.
	CISA Releases IOCs Associated with Malicious Barracuda Activity (08/29/2023) - CISA has released additional indicators of compromise (IOCs) associated with exploitation of CVE-2023-2868. CVE-2023-2868 is a remote command injection vulnerability affecting Barracuda Email Security Gateway (ESG) Appliance, versions 5.1.3.001-9.2.0.006. Malicious threat actors exploited this vulnerability as a zero day as early as October 2022 to gain access to ESG appliances. Download the newly released IOCs associated with this activity: IOCs Associated with Exploitation of Barracuda ESG Vulnerability CVE-2023-2868 (JSON, 85.34 KB) Review the following advisories for more information: • Barracuda: Barracuda Email Security Gateway Appliance (ESG) Vulnerability • Mandiant: Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868) See CISA Releases Malware Analysis Reports on Barracuda Backdoors for malware analysis reports (MARs) covering previously released IOCs and YARA rules and Barracuda Networks Releases Update to Address ESG Vulnerability. ***Comment: Barracuda revealed that the attackers exploited the CVE-2023-2868 remote command injection zero-day to drop previously unknown malware dubbed Saltwater and SeaSpy and a malicious tool called SeaSide to establish reverse shells for easy remote access.***

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