Bank Monitoring and Reporting Obligations Regarding
Elder Financial Exploitation:
Brief Overview of Major Federal and State Laws and Regulations

There are a number of federal laws and regulations concerning bank obligations regarding detecting Elder Financial Exploitation (EFE). The following is a summary of some of the major requirements:

- Red Flag Rule: Requires banks to develop a written identity theft prevention program to identify and address identity theft.
- Anti-Money Laundering (AML) - Bank Secrecy Act (BSA): Requires banks to develop AML programs, including internal policies, procedures, and controls to detect and report suspicious transactions and activities.
- Customer Identification Program (CIP) - Bank Secrecy Act (BSA): Requires banks to have risk-based procedures to identity of their customers.
- Regulation E and Regulation Z: Protects consumers using cards and other electronic payments by establishing disclosure requirements, procedures for resolving errors, and limitations to consumer liability for unauthorized activity.

1. Fair Credit Reporting Act (FCRA) Red Flag Rule

The rule requires banks to develop and implement a written Identity Theft Prevention Program (ITPP) to recognize and address identity theft red flags. The program must be appropriate to the size and complexity of the financial institution and the nature and scope of their activities. The bank's board of directors must approve the program, as well as be involved in its oversight, development, implementation, and administration.

Entities subject to the Rule must:

- **Identify relevant flags**: Establish procedures to recognize suspicious patterns or activities that may indicate identity theft.
- **Detect Red Flags**: Implement systems to spot warning signs during day-to-day operations.
- **Respond appropriately**: Take action to prevent and mitigate identity theft when red flags are detected.
- **Update their program**: Review and update programs to reflect changes in identity theft risks and ensure effectiveness.

The Oregon Banker's Association has a link to the ABA's "14 Red Flags for Elder Financial Abuse" on their website under "Community Resources/ Protecting Seniors from Financial Exploitation" page.

2. Anti-Money Laundering (AML): Bank Secrecy Act (BSA) & USA PATRIOT Act

The BSA aims to prevent money laundering and other financial crimes by requiring banks to report certain transactions and maintain records. Its key provisions are:

- **Reporting Requirements**: Banks must file reports for cash transactions exceeding $10,000 and report any suspicious activities indicating money laundering or other criminal activities.
- **Record Keeping**: Banks must maintain records of cash purchases of negotiable instruments and other relevant transactions to facilitate investigations by law enforcement.
- **AML Programs**: Banks must establish AML programs, which include internal policies, procedures, and controls to detect and report suspicious activities. This includes internal controls to assure ongoing compliance, training for appropriate personnel, and risk-based procedures for conducting ongoing customer due diligence.
- **Compliance and Enforcement**: The Financial Crimes Enforcement Network (FinCEN) oversees the implementation of the BSA, ensuring Banks comply with its requirements.
- **Advisories**: FinCEN released their "Advisory on Elder Financial Exploitation EFE" on June 15th, 2022 which reminds Banks of their relevant BSA obligations and tools:
    - **Suspicious Activity Reporting (SAR)**: Banks must file a SAR if detected activity involving the use of the bank to facilitate criminal activity, including EFE. The SAR form has a check box specifically for EFE.
    - **Currency Transaction Reporting (CTR)**: Obligations to report cash payment over $10,000. For transaction related to EFE, banks must include specific comments.
    - **Information Sharing** for banks under the safe harbor provided under the USA PATRIOT Act section 314(b)

Banks use AML software to comply with BSA's rigorous monitoring and reporting requirements. These systems use data analytics, artificial intelligence, and machine learning for detecting financial crime. All include monitoring specifically aimed at identifying potential EFE transactions.

3. Customer Identification Program (CIP): Bank Secrecy Act (BSA)

BSA CIP requires banks to have risk-based procedures to form a reasonable belief that they know the true identity of the customers. Key requirements are:

- **Verify customer identity** to form a reasonable belief they know their customers.
- **Collect identifying information** including name, date of birth, address, and Identification number (TIN/SSN)
- **Verification methods** using documentary methods and non-documentary methods.
- **Recordkeeping** of the information maintained and verification methods.
- **Government list checks**, such as OFAC

4. Regulation E and Regulation Z

Regulation E implements the Electronic Fund Transaction Act (EFTA), which protects consumers when they use electronic funds transfers (EFTs) such as debit cards, online Banking transfers, and Automated Clearing House (ACH) transfers. It requires banks to provide clear disclosures, establishes procedures for resolving errors, and limits consumer liability for unauthorized activity. Types of transactions covered include:

- ATM transactions
- Direct Deposits
- Debit Card purchases (point-of-sale)
- Prepaid cards
- ACH transfers
- Remote banking programs.

Disputes for Credit Cards are covered under Regulation Z, the Fair Credit Billing Act which give consumers the right to dispute billing errors, requires card issuers to investigate, and limits consumers liability for unauthorized transactions. Consumer liability for unauthorized transactions under both Regulations E and Z must be disclosed by banks at the time a consumer contracts for a card or related service, or before the first EFT is made from their checking/savings account. Card issuers utilize robust fraud monitoring and customer notification software to identify, confirm, and manage potentially fraudulent card transactions.

* * * * *

In addition to some of the federal laws and regulations listed above, Oregon has also been active in providing banks with tools to help stop EFE. The following are two provisions that allow banks to communicate with authorities and to place a temporary hold on an account when EFE is suspected.

5. ORS 708A.675 Account Hold

ORS 708A.675, a statute in the Oregon Bank Act that permits a bank to place a temporary hold on an account if EFE is suspected, was a measure passed by the Legislature in 2017 and introduced at the behest of the Oregon Bankers Association. Oregon was one of the first states in the county to implement an account hold provision and it provides banks with the ability to place a 15 day hold on a transaction if the bank has a reasonable belief that a vulnerable person (which includes an elderly individual) may be subject to EFE.

6. ORS 192.586 Outreach to State and Local Law Enforcement

ORS 192.586 is a provision that permits a bank, in its discretion, to initiate contact with state and local agencies concerning a suspected violation of law, including EFE. This is a tool that is utilized by banks in which suspected EFE is suspected. This statute was last amended in 2013.

If you have any questions, please feel free to contact OBA Government Affairs Director Kevin Christiansen at (503) 576-4123 or our lobbyist John Powell at (503) 510-8758.