Banking Compliance

BAI Learning Courses

Index

* *BSA and AML: Essentials.*
* *Developing a Complaint Management Policy [Mini-Course].*
* *Unfair, Deceptive, and Abusive Acts or Practices (UDAAP): Mitigating Risk.*
* *Regulation CC: Essentials.*
* *Reg E: Handling Errors and Complaints.*
* *Frontline: Marketing & Social Media.*
* *Contact Center: Handling Complaints.*
* *Contact Center: Marketing Rules & Social Media.*
* *Reg D: Convenient Withdrawals [Mini-Course].*
* *SAR: Responding to Suspicious Activity.*
* *CCPA (California Consumer Privacy Act) [Mini-Course]*

#

#

#

#

#

#

#

#

#

# —

# BSA & AML: Essentials

Preparing against money laundering and fraudulent activities.

BSA: The Bank Secrecy Act

Design to detect/prevent illegal activities.

*Patriot Act 2001*: add focus on combatting terrorism.

Money Laundering

The exchange of dirty funds for clean money. Using transactions to cover up a long trail of illegal funds.

Three (3) stages

* *Placement*: financial institution or the retail space.
* *Layering*: complex transactions to hide where the funds originated.
* *Integration*: the funds re-enter the economy.

Causes of Money Laundering: financial fraud, drug trafficking, tax evasion, illegal arms sales, foreign official corruption, terrorist financing, computer crimes, smuggling, and currency exchanges.

 USA PATRIOT ACT - Information Request

* *314 (a) Request*: sharing information with law enforcement agencies.
* *314 (b) Request*: sharing information with other financial institutions.

BSA Violations

* Knowingly failing to collect or verify CPI information.
* Knowingly neglecting to complete and file a SAR when it’s necessary.
* Knowingly neglecting to complete and file a CTR when it’s necessary.
* Knowingly completing a wire transfer or selling negotiable instruments when either transaction involves $3,000 or more and failing to collect and verify customer and transaction information.

Penalties: probation, termination, removal of employment in the financial services industry, jail time, and monetary penalties.

\*When in doubt, always ask questions to your supervisor.

Customer Identification Program (CIP)

The exchange of dirty funds for clean money. Using transactions to cover up a long trail of illegal funds.

The CDD Rule: Customer Due Diligence (CDD) Requirements were established in 2016 to identify and verify the beneficial owners of legal entity customers.

Beneficial owner

* Each individual who directly or indirectly owns 25% or more of the equity interests of a legal entity customer (i.e. “the ownership prong”).
* A single individual with significant responsibility to control, manage, or direct legal entity customers, including an executive officer or senior manager or any other individual who regularly performs similar functions (i.e “the control prong”).

A legal entity will have up to five (5) beneficial owners - one (1) person under the control prong and zero to four (0-4) persons under the ownership prong.

Required Information: Name, DOB, Address, SSN (or other).

Compliance: for any new accounts including new accounts for existing customers.

Mandatory: verify that the information is genuine.

* + - * Documentary methods.
			* Non-Documentary methods: checking unexpired government-issued ID. And when it comes to businesses, certified articles of incorporation or a government-issued license may be checked, also a “certificate of good standing” through the Secretary of State.

 OFAC List

*Specially designated Nationals (SDN) and Blocked Persons List:* contains the names of alleged drug traffickers, terrorists, terrorist organizations, and/or individuals affiliated with the government or acting on behalf of an entity or nation.

*Customer Due Diligence (CDD):* predicts the types of transactions in which a customer is likely to engage, which assists in determining when transactions are potentially suspicious.

Customer Due Diligence (CDD): predicts the types of transactions in which a customer is likely to engage, which assists in determining when transactions are potentially suspicious.

Doing it effectively

* Detecting and reporting suspicious transactions.
* Avoiding criminal exposure from persons who use or attempt to use the institution's products and services for illicit purposes.
* Adhering to safe and sound banking practices.

Enhanced Due Diligence (EDD): frequently monitoring high-risk customer relationships.

 *High-risk factors:*

* Transaction account history with the institution.
* Geographic location of transactions.
* Attributes of the business.
* Expected and actual cash and fund transfer activity level.
* SAR history.
* Law enforcement agency inquiries.
* 90 days first new accounts.
* High-risk areas, entities and businesses.
* Others.

Currency Transaction Report (CTR)

It is mandatory. More than $10,000 of cash transactions (deposits, withdrawals, loan payments, negotiable instruments purchase, and currency exchanges).

*Rules:*

* Transactions may be conducted by an individual or someone acting on behalf of the individual.
* Transactions may take place at one branch or multiple branch locations.
* Transactions occur in one business day.
* There can be one cash transaction or multiple cash transactions that add up to more than $10.000 in that business day.

How does the BSA Define One Business Day? e.g. after the cut-off time on Wednesday. Then on the next morning. It is the same business day.

CTR Parts:

* Information on the person(s) involved in the transaction(s).
* Amount and type(s) of transaction(s) that took place.
* Information of the financial institution where the transaction(s) took place.
* Information of the filing financial institution - which is usually, but not limited to, the institution where the transaction took place.

CTR Exemptions:

* *Phase I*
	+ Financial institutions.
	+ Departments and agencies of the U.S.
	+ Any entity listed on the NY Stock Exchange (NYSE) or other national exchanges
	+ NASDAQ National Market Security designated company.
* *Phase II* - may be granted an exemption if they meet the following criteria:
	+ The entity has maintained a transaction account for 2 months or a risk-based analysis completed. Showed a legitimate business purpose for conducting frequent large currency transactions.
	+ Exceeded 10K cash transactions at least 5 times during the last twelve months.
	+ Incorporated/organized under U.S/state laws and registered/eligible to do business within the U.S. or a state.
* *Phase III* - payroll purposes if they meet the following criteria:
	+ The entity has maintained a transaction account for 2 months or a risk-based analysis completed. Showed a legitimate business purpose for conducting frequent large currency transactions.
	+ Frequently withdraws more than 10K to pay U.S. employees in cash.
	+ Incorporated/organized under U.S/state laws and registered/eligible to do business within the U.S. or a state.

$3,000 rule: in cash when is involved in a negotiable instrument purchase, a funds transfer, or a third party transfer. Like traveler’s check, wire transfer, etc. Regardless of payment method.

Negotiable Instruments: bank check, cashier’s check, traveler’s check, money order.

Existing Deposit Accounts: name of purchaser (primary ID), date of the purchase, type of instrument(s) purchased, serial number of each of the instruments, dollar amount of each of the instruments purchased in currency, specific identifying information, e.g. through a signature card, record, or primary ID. Everything needs to be CURRENT.

No Account Relationship Established: name and address of the purchaser, SSN or Alien number, DOB, date, type of instrument used, serial numbers of each instrument, dollar amount of each instrument, specific identifying information, e.g. through a signature card, record, or primary ID. Everything needs to be CURRENT.

Funds and Wire Transfers: for customers and non-customers.

* *Established Customer Information:* name and address of the originator, amount of the payment order, date of the payment order, any payment instructions, identity of the beneficiary's institution, beneficiary (any of these: name, address, account numbers or others).
* *Non-Established Customer Information:* name and address of the originator, amount/date of the payment order, any payment instructions, identity of the beneficiary’s institution, beneficiary (any of these: name, address, account numbers or others), name/address of the person placing the order, type of identification reviewed, number of identification document, TIN, SSN, EIN, AIN, Passport number and country of issuance. Everything needs to be CURRENT.

Recordkeeping Requirements: records must be retained for a period of five years (or longer if state law requires it). May be retained as originals, copies, and/or electronic records.

Fund Transfers + OFAC List: financial institutions are required to check all new wire transfer originators and beneficiaries against the OFAC list. Both incoming and outgoing wires.

REPORTING: Suspicious Activity Report (SAR).

*Structuring* (federal crime): spacing of transactions for illicit purposes.

All financial institution staff need to be alert to anything that may seem suspicious or out of the ordinary. When in doubt, report it immediately.

*Safe harbor:* federal law protects from civil liability to the institutions and its directors, officers, employees, and agents that make a disclosure of any possible violation of law and regulation.

Requirements

*Maintain it confidential:* under threat of monetary penalties. Just the designated supervisor of the department unless the situation involves a witness or a coworker. Exception: law enforcement agencies and other companies for BSA monitoring purposes. Safe Harbor can be revoked.

Provide detailed information: who, what, where, when, why, and how?

*Elder Financial Exploitation:* include the term in the narrative portion of all relevant SARs filed. The narrative should also include an explanation of why the institution knows, suspects, or has a reason to suspect that the activity is suspicious. The victim of elder financial exploitation should not be reported as the subject of the SAR, but all its information should be included.

Medicare Fraud Schemes

* Account
* Payments
* Detection
* Loss

FBI + FinCEN asked financial institutions to file a SAR and call the FBI (310) 477-6586 when they open business accounts by *individuals that meet the following description*:

* Under 30 and attempt to open a business account.
* In the U.S. on a J-1 Visa.
* Use a state ID or passport instead of a driver’s license to fulfill CIP requirements.

# —

# Developing a Complaint Management Policy

The role of complaint management: crucial function of any compliance management system (CMS). Provides a significant amount of data when an institution is performing a risk assessment, reviewing the effectiveness of a new product or service, and ensuring compliance with regulations.

1. Define what the institution considers a complaint: learn how to distinguish between legitimate from frivolous complaints.
2. Implement an escalation process for complaints: to ensure that the consumer receives appropriate attention and an adequate response from management.
3. Designate a centralized point of contact: to ensure that customers receive a consistent and fair response from the institution.
4. Use a complaint log: nature of the complaint, date when the complaint was received, how the complaint was resolved, the root cause of the complaint, length of time to resolve the complaint, who resolved the complaint, the complainant’s name, how the complaint was received (email, social media, regulatory agency, etc).
5. Ensure timely responses: to show both the complainants and regulatory agencies that complaint management is important to the institution.
6. Define how the institution will analyze complaints for trends and patterns: identify situations that indicate weaknesses in the CMS program that may lead to consumer harm or compliance violations (fair lending concerns, unfair/deceptive/abusive acts or practices concerns, issues related to a specific employee or department, system processing issues).
7. Report results to senior management and the board of directors: the complaint log, along with any supporting analysis, should be submitted regularly to the senior management and the board of directors for review.

—

# Unfair, Deceptive, and Abusive Acts or Practices (UDAAP): Mitigation Risk

Financial institutions (and its employees) have the legal obligation to protect their consumers from UDAAPs.

This can cause:

* Substantial financial injury to customers.
* Destroy consumer’s confidence in financial institutions.
* Damage the financial marketplace.

Dodd-Frank Wall Street Reform + Consumer Protection Act: it is unlawful to engage in UDAAPs.

Consumer Financial Protection Bureau: creates and enforces rules to prevent UDAAPs.

Unfair Acts & Practices

* *It causes or is likely to cause substantial injury to consumers:* monetary harm, fees of an unfair practice, even if it’s a small amount of harm to a large number of people.
* *The injury is not reasonably avoidable by consumers:* when the act/practice interferes with the consumer’s ability to make an informed decision or to take action to avoid injury. Like pricing information is missing from an advertisement.
* *The injury is not outweighed by any benefits to consumers:* if the net of an act/practice results in harm to consumers. (e.g. when an account boasts ‘no annual fees’ but requires other fees and charges that outweigh this benefit).

Examples

* Refusing to release lien after the consumer makes their final payment.
* Dishonoring credit card convenience checks without notice.
* Processing payments for companies engaged in fraudulent activities.

Deceptive Acts/Practices

* The act or practice misleads or is likely to mislead consumers: by representation or by omission (e.g. offering fee structures that are not truly available).
* A reasonable consumer would be misled: consumer’s interpretation of the omission, representation, act, or practice.
* The misleading act or practice is material: likely to affect the consumer’s choice or conduct regarding the product or service. Material: costs, benefits, restrictions.

Examples

* Inadequate disclosure of material lease terms in television advertising.
* Misrepresentation of loan terms.

Abusive Acts/Practices

* Materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service.
* Takes unreasonable advantage of the consumer: 1) Lack of understanding by the consumer of the material risks, costs, or conditions of the product/service. 2) Inability of the consumer to protect their interest in selecting or using a financial product or service. 3) The reasonable reliance by the consumer on a covered person to act in the interest of the consumer.

Other Laws: TILA, TISA, ECOA, FHA, FDCPA, FCRA.

*TILA (Regulation Z):* specific disclosure and advertisement requirements for consumer lending. Amendment: lenders need to consider a consumer’s ability to repay (ATR) when underwriting mortgages. Loan terms need to be understandable, not unfair, not deceptive, not abusive.

*ECOA*: prohibits discrimination of a credit transaction against a consumer based on race, religion, color, national origin, sex, marital status, age, income, or has excercised their right under the CCPA.

*FHA*: prohibits creditors involved in a residential real estate transaction from discriminating against a consumer based on race, color, religion, sex, disability, familial status, or national origin.

Mitigating UDAAP Risk.

* Compliance Self-Assessment: UDAAPs can occur at any stage of the credit lifecycle - Sales & MKT, Underwriting and Account Origination, Account Management and Loan Servicing, and Collections.
* Institutions should ask themselves:
	+ How is the selection process handled?
	+ Are consumers given a choice of products and services?
	+ What happens if new and more beneficial products are introduced after consumers are already utilizing a more expensive option?
	+ Is the T & C of a product simple or complex?
	+ What acts or omissions might interfere with consumers’ understanding? How will the institution measure the consumer’s availability to understand?
	+ Know the target audience.

*Consumer Complaints:* to detect UDAAPs. Consumers may file complaints with the institution itself, the Better Business Bureau, the CFPB, or other entities. Through an effective complaint management system, the institution can analyze complaints for trends and review its practices to avoid UDAAP violations.

Potential Targets

* *Credit Life Insurance: the Dodd-Frank Act:* prohibits creditors from financing single-premium credit life insurance directly or indirectly with any residential mortgage loan or HELOC. These institutions should ensure that consumers are receiving sufficient information to make an informed decision as to whether this product is right for them.
* *Punitive Mortgage Loan Provisions:* include negative amortization and prepayment penalties and may also include such normal practices as certain variable rate features and balloon payments. They aren’t inherently abusive but if consumers don’t fully understand the risks associated with these products, it’s a risk.
* *ATM and Overdraft Feeds:* institutions generally cannot overcharge fees without a customer’s prior authorization. Outrageous fees could expose the institution to UDAAP scrutiny.
* Third-Party Products: like credit protection or identity monitoring offered by a third party vendor for a monthly fee/membership. The institution is responsible for it anyways.

MKT Programs, Advertisements, and Other Promotions need to:

* All representations are factually based.
* Disclosures are clear and conspicuous and include costs, benefits, availability, fees, penalties, and other T&Cs.
* Inform customers with key terms that are important to make an informed decision.
* Avoid terms that are generally not available to the target audience.
* Costs, conditions, and other terms are not misrepresented, either explicitly or by omission.

*Fee Income and Compensation Models*: it’s not forbidden but they shouldn’t be a temptation to deceive or mislead consumers. They can be reviewed to determine if the fee income was earned abusively (from overdrafts or prepayment penalties).

*Debt Collection and Credit Reporting*: financial institutions may also be held responsible for unfair, deceptive, or abusive debt collection acts or practices (including by third-party collectors).

 —

# Regulation CC: Essentials

Federal Reserve Board

Expedited Funds Availability Act (EFAA): enacted by the Congress in 1987.

Before Regulation CC: financial institutions could delay the availability of funds for a deposit for any length of time and had no legal obligation to inform customers when they would be able to access their money.

EFAA and Regulation CC: Congress established the EFAA implemented by the Federal Reserve Board’s Regulation CC, to apply both consumer and commercial transactions accounts. Regulation CC does not cover savings, money market, or time deposit accounts.

(3) major provisions to protect depositors and financial institutions:

* Limit the length of time for holds placed on deposits.
* Disclose specific availability policies in a timely manner.
* Accrue interest on unavailable funds deposited to an interest-bearing account, no later than the business day the institution receives credit for the funds.

Regulation CC specifies the business day by which each type of deposit must become available to the depositor for withdrawal. It’s up to each financial institution to implement its own funds availability policy that falls within these limits.

How to disclose the funds availability policy:

* Lobbies of all branches.
* Where deposits are accepted including ATMs.
* On the front of the preprinted deposit slips.
* At the time of account opening in a manner that the customer can keep.

Next Day Availability - the following types of deposits must be made available on the next business day following the day of deposit.

* *Cash*: that’s deposited in person to an employee of the financial institution.
* Electronic payments: on the next business day following receipt (no the day the transfer is sent).
* *U.S. Treasury checks*: regardless of the method of deposit.
* *U.S. Postal Service money orders*: that are deposited in person to an employee of the financial institution and into an account held by the payee.
* *Federal Home Loan Bank or Federal Reserve Bank checks*: that are deposited in person to an employee of the financial institution and into an account held by the payee.
* *State or local government checks*: that are deposited in person to an employee of the financial institution and into an account held by the payee. Please note that some financial institutions may also require the use of a special deposit slip to receive next-day availability.
* *Cashier’s, certified, teller’s checks*: that are deposited in person to an employee of the financial institution and into account held by the payee. Please note that some financial institutions may also require the use of a special deposit slip to receive next-day availability.
* *On-us checks*: drawn on and deposited into accounts at the same financial institution. On-us checks must be deposited in person to an employee of the institution or at an on-site ATM to receive next-day availability.

Two-Day Availability - deposits made at nonproprietary ATMs must be made available by the fifth business day.

Delaying the Availability of Funds.

* *Case-by-Case Holds:* the first $225 of the held deposit must be made available by the next business day.
* *Exception Holds:* when it represents a higher level of risk to the financial institution, for a “reasonable period of time” (typically defined as one additional business day for on-us checks - total of 2 business days) and five additional business days for other checks (total of seven business days). No applicable to cash and electronic payments.
	+ *New Accounts:* present an unknown degree of risk. An account is considered new if each individual on the account has not had a transaction account at the institution within the previous 30 days, for a period of at least 30 days. For new customers, only the first $5525 of next-day items qualifies for next-day availability The amount over $5525 must be made available by the ninth business day after the day of deposit. For other check deposits, a financial institution may decide on any availability schedule.
	+ *Large Deposits:* when it exceeds $5525 the over amount may be held according to the “reasonable” timelines.
	+ *Redeposited Checks:* when a check is returned and then redeposited, there is a greater risk to the financial institution of the funds being uncollectible a second time. The full amount of the deposited item may be held according to the timelines. Doesn’t apply to a check that was re-deposited because it was returned due to a missing endorsement or because it was postdated.
	+ *Repeat Overdraft Accounts:* an account must be overdrawn or would have been overdrawn if checks had not been returned - 1) for six or more business days during the previous six months; 2) by at least $5525 on two or more business days in the past six months.
	+ *Reasonable Cause to Doubt Collectibility:*  because the check is more than six months old or because the paying institution has sent a stop payment notice.
	+ *Emergency Conditions:* rarely used. Checks that are deposited during situations outside the financial institution’s control (power failure, natural disaster). May be held for any length of time as long as the institution can justify the hold.

Notifications for Holds on Deposits: the account holder must be notified in writing. At the time of deposit or mailed or delivered no later than the first business day following the banking day the deposit was made.

—

Reg E: Handling Errors and Complaints

Financial institutions have teng (10) business days to investigate an error or complaint.

*\*Written notifications are not required.*

* *EFT Education:* familiarise yourself with different types of EFTs handled by the institution so we know when an error/complaint comes under the jurisdiction of Reg E.
* *Recognize Errors:* so they get logged/investigated within the permitted timeframes.
* *Reg E Contact or Department:* know who’s in charge of Reg E error resolution at your institution. This person/department will log the EFT error, begin the investigation immediately, and ensure that action is taken and communicated in the permitted timeframes.
* *Oral Notice:* don’t wait for written notice.

What is an error?

* Unauthorized EFT.
* Incorrect EFT.
* Omission of EFT on a Periodic statement.
* Computer or bookkeeping errors.
* Wrong amount of money issued at an electronic terminal.
* Improper Identification of EFT.

What is not an EFT Error? (these situations don’t require investigation).

* Routine Balance Inquiries: e.g. verification of account balance.
* Routine Complaints: e.g. complaint about fees for being too expensive.
* Duplicate Document Requests: e.g. someone asks for copies of statements twice.
* Consumer Requests for Tax or Recordkeeping Purposes.

Reg E Contact or Department: most financial institutions have either one person o a central group to handle potential errors and complaints, to guarantee that errors are properly recorded, tracked, and processed in the required timeframes.

EFT Error Log: the contact/group should be responsible for maintaining a log of all EFT errors and alleged EFT errors. The should capture:

* The individual, office, or department handling the complaint.
* The individual assigned to investigate the error.
* The date the error, notification, or complaint was received.
* Whether the deadlines for error resolution were met.

Most financial institutions used a standardized Reg E inquiry/complaint form.

What consumers must report: must provide the institution with enough information to identify the account and the name on the account. If the actual account number is not provided, a SSN or some other unique identifier is enough. Consumers must provide as much detail as possible about the suspected error, such as the amount involved and the date it occurred.

Liability and Consumer Reporting Timeframes: the financial institution must receive the allegation of error no more than 60 days after the institution issued the periodic statement containing the error. For payroll card accounts, an error report is ‘timely’ when it’s made within 60 days of either:

* The date the consumer accesses the EFT history that includes the disputed transaction.
* The date the financial institution sends the written history that includes the disputed transaction.

*\*Financial institutions must investigate all error allegations related to unauthorized transactions before imposing any liability.*

EFT Error Investigation Timelines.

* *When an account is not provisionally credited:* must promptly investigate any alleged error and reveal the findings within 10 business days of being notified of the error. It should be corrected no more than 1 business day later. The institution must report the results of its investigation to the consumer within 3 business days of concluding the investigation.
* *When an account is provisionally credited:* the institution may take 45 calendar days to investigate an error only if it meets the following requirements 1) the consumer’s account is provisionally credited for the disputed amount within 10 business days. 2) The consumer has access to provisionally credited money during the investigation. 3) Within 2 business days of the provisional credit, the consumer must be notified (orally or in writing) of the amount, the date of the credit and the fact that the consumer does have access to those funds during the length of the investigation.
* *Foreign and POS Debit Card Transactions:* financial institutions have more time to investigate if: 1) An EFT was not initiated in a state (PR, District of Columbia, or any territory or possession of the U.S.) 2) It’s a POS card transaction. It may take up to 90 calendar days if it provisionally credits the consumer’s account with the disputed amount within 10 business days.
* *Transactions Involving a New Account:* within 30 days of the first deposit to the affected account, the institution must determine whether or not an error occurred within 20 business days of receipt of the notice. For new accounts disputes, a 90-calendar-day period applies for the investigation if the institution provisionally credits the consumer’s account within 20 business days. The institution must disclose this information to the consumer.
* Transactions Involving Extensions of Credit: Reg Z (Truth in Lending) billing error resolution requirements may apply - if a transaction has both EFT and credit aspects, then Reg E controls the transaction, and Reg Z applies only to the credit-related aspects of the situation that Reg E doesn’t cover. (e.g $20 withdrawal and receiving $200 causing and overdraft - extension of credit).

EFT Error Investigation FAQs

What if your institution requires written confirmation?

If the consumer fails to respond to that request within 10 business days, the institution can take 45 calendar days and not provisionally credit the consumer’s account.

If there’s a dispute about a POS, foreign, or new account transaction, and if written confirmation is not received, an institution can take 90 calendar days to investigate without provisionally crediting the account for the dispute amount.

*Two requirements (or they might be violating Reg E):*

1. The consumer must be informed of the written confirmation requirement at the time “notice” is given. And provide the address of where to send it.
2. A consumer’s written notice should be considered “given” at the time the consumer mails the notice or delivers it to the institution.

What if the consumer was wrong and the account was already provisionally credited?

No error is discovered within the 45-day timeframe, an institution may remove the funds from the customer’s account but must notify the consumer of the date and the amount to be removed.

For 5 business days, the institution can’t charge an overdraft fee but after that period, your institution can refuse POS transactions and charge the fee.

If during the 5 business days after transmitting the notice, the consumer attempts a transaction that would have resulted in an overdraft even if the credited funds were still on deposit, then your institution doesn’t have to honor the transaction.

What if a consumer withdraws an error?

If a consumer withdraws a notice of error before the investigation is completed, the institution should mark these withdrawals clearly in the institution’s records.

If proper documentation is not carried out, it may appear that the institution has violated Reg E by failing to properly conclude the investigation.

Communicating the Results of the Investigation.

It should be communicated to the consumer and the Reg E contact or department (if the investigation was handled by another individual). With sufficient internal documentation.

Investigation Findings: the consumer shall be given a written explanation of the findings noting the right to request documentation used to make the determination. If requested, it should be provided promptly.

Error Investigations and Third-Party Records: an institution is required to investigate an error only as far as it can by using its own records. Institutions are not required to obtain records from third parties to determine what may have happened.

 —

# Frontline: Marketing & Social Media

Marketing & Advertising

Advertising is the type of marketing that is regulated for the protection of consumers, both in a general sense and specifically for financial products.

As frontline employees, it is important to be familiar with the advertisements that bring customers and what actions might be taken as advertising.

We should be able to:

* Answer questions and make an initial response to complaints about advertising.
* Direct consumers to the right person or resource for more information about advertised products.

Avoiding UDAAP

Unfair Advertising:

* It is likely to cause substantial monetary losses; to any number of individuals, or a smaller loss to a substantial number of individuals.
* The loss cannot reasonably be avoided, perhaps because a key disclosure was left out of an advertisement.
* The loss is not outweighed by a related gain.

Deceptive Advertising:

* It is misleading to a reasonable consumer. The consumer’s interpretation is more important than the advertiser’s intention (e.g. an exaggeration).
* The advertisement is likely to affect an actual choice regarding a product or service.

Abusive Advertising:

* Interferes with the consumer’s ability to understand the terms and conditions of the product.
* Takes advantage of the consumer’s lack of understanding of the risks or potential costs of the product, and their trust in the advertiser to act on his/her best interest.

 Prohibited Ads:

* *Bait and Switch:* deceives customers into believing that they will be able to get a better deal than they can in fact receive.
* *No-cost or Free Accounts:* even though activity fees or maintenance fees are nonexistent, they can get charged for check reorders fees, non-sufficient funds fees, or dormancy fees.
* *Profit on Accounts:* the word “profit” cannot be used to characterize interest or earnings on an account.

Triggering Terms for Deposit Accounts: using them triggers the inclusion of additional explanations or disclosures.

* Annual Percentage Yield (APY) - triggers a requirement that the following must be shown clearly and conspicuously in the advertisement:
	+ The period of time of the APY is in effect, or a statement that the APY is accurate as of a specified date.
	+ Any minimum balance required to earn the advertised APY, as well as the minimum balance to open the account (if it is greater).
	+ A statement that fees could reduce earnings on the account.
	+ For ***time accounts***, the length of time the account must be open to earn the advertised APY, as well as a statement noting that an early withdrawal penalty may or will be imposed.
	+ For ***variable rate accounts***, a statement that the rate may change after the account is opened.
	+ For ***tiered accounts paying different rates*** depending on the account balance, the minimum balance for each tier must be shown near and with equal prominence to the applicable APY.
* Bonus - if a bonus premium, gift, award, or other consideration worth over $10 in cost to the institution is advertised, it must include:
	+ The APY.
	+ Any minimum balance requirements, either for opening or maintaining the account, that are required to receive the bonus.
	+ Any time requirement to receive the bonus.
	+ When the bonus will be provided.
* Overdraft Protection - does not apply to arrangements to transfer funds from another deposit account or a formal overdraft line of credit, even if a fee is charged for such transfers (e.g. a savings account linked to a checking account is overdrawn, so funds are automatically transferred from the savings account to cover the difference) .It must include:
	+ The fee or fees charged for paying each overdraft.
	+ The categories of transaction (check, pre-authorized debit, etc) that can lead to an overdraft fee.
	+ The time period by which the consumer must repay any overdraft.
	+ Any exclusions when overdraft protection will not be paid.
* Exceptions - lawmakers realize there is not always enough time or space in an advertisement to include all of these disclosures.
	+ Broadcast media (TV, radio), outdoor billboards, telephone response machines, and signs inside a depository institution, may have exceptions to these rules.
	+ Online advertisements or sent by email are considered equivalent to written advertisements, since consumers have time to review all required disclosures.
	+ When the electronic advertisement is done through audio or video, printable disclosures may still be linked to the advertisements.

Phone, Email, and Social Media.

* Phone and email Solicitation:
	+ ***Do Not Call:***
		- You cannot solicit by calling personal phone numbers, including cell phone numbers, that are on the registry.
		- “Robocalls” may not be made without prior express written consent from the consumer. They must include an automated, interactive opt-out feature enabling consumers to immediately end such calls.
		- The financial institution must maintain a list of do-not-call numbers that includes the National Do-Not-Call registry, any similar State registry, and any consumers who have personally asked to be excluded from phone solicitation. The financial institution is responsible for checking the official lists for additions and changes at least every 31 days.
		- Exception: for customers with which it has an existing business relationship but it should still keep an internal list of consumers who have asked not to receive solicitation calls.
	+ *CAN-SPAM* - Controlling the Assault of Non-Solicited Pornography and Marketing Act was passed in 2003. This law covers solicitation emails only. The unsolicited email message must meet the following criteria:
		- They cannot contain false or misleading information in the “To” and “From” fields.
		- They can’t have deceptive subject lines.
		- They must be clearly identified as ads.
		- They must contain information on where your institution is located.
		- They must provide recipients with a way to opt out of future emails.
		- The institution must:
			* Respond promptly to opt-out requests.
			* Monitor that vendors send on the institution’s behalf.
* Social Media and Marketing: includes blogs, picture-sharing, vlogs, wall-postings, email, instant messaging, music-sharing, crowdsourcing, and voice over IP. Guidelines to be followed:
	+ Most things you post online can be seen by members of the public beyond your own circle of friends and acquaintances.
	+ Do not use your social media accounts to advertise your institution’s products or services.
	+ Consider what you post on your personal accounts as a reflection of the institution, particularly if that content can be traced back to you as an employee of your institution.

 —

# Contact Center: Handling Complaints

Identifying Complaints

* Written: can be a letter or email sent by a consumer to the financial institution. Letters are often addressed to retail branches since they have the most consumer contact. Complaints may also be included in payment envelopes. Employees who monitor general email inboxes should review emails for complaints and know the process for reporting them.
* Verbal: contact centers, loan servicing personnel, and branch employees are some of the most frequently contacted groups in the institution. All staff members should be aware of what constitutes a legitimate complaint and the process for reporting such complaints to management.
* Regulatory agencies: consumers can easily log complaints on the CFPB website, which are then available for public review by institution name. Complaints received through other regulatory agencies are logged within that agency but are not publicly available. Any complaints received by a regulatory agency during an examination period will be considered and can affect the exam rating and/or compliance findings of an institution.
* Social Media and Internet: as Facebook and Twitter, and review websites such as Yelp or the Better Business Bureau, can be a channel for consumers to voice complaints. Even if an institution has a “no social media” policy, it’s still in the institution’s best interest to monitor social media sites, as employees and consumers alike can post information relating to the institution.

Complaints, Disputes, or Feedback

Determine the urgency of response by identifying if it is a complaint, a dispute, or just negative feedback.

* *Complaints*: demands a response in a certain manner. Can be logged/used for analyzing trends by your leadership, or they can mean serious consequences for the institution. Can revolve around a product or service not functioning like it’s supposed to or can be as severe as discriminatory behaviour.
* *Disputes*: if a consumer finds an error, disagrees with billing, or disagrees with your institution’s filing with a consumer reporting agency, he or she may initiate a dispute. For borrowers, this is important because inaccurate consumer reports may affect their ability to obtain credit, get an apartment, or even a job that requires a credit report.
* *Negative Feedback*: the institution has done nothing wrong, or the error has little consequence on the consumer.

Complaint Management

* *Implement an escalation process*: to define how complaints will move up the command chain to ensure that the consumer receives appropriate attention and an adequate response from management.
* *Designate a centralized point of contact*: to ensure consumers receive a consistent and fair response from the institution.
* *Utilize a complaint log*: during a compliance examination, examiners will often review a complaint log as part of the overall CMS assessment.
* *Ensure timely responses:* to show both the complainants and regulatory agencies that complaint management is important to your institution.

Discussions with the Consumer

* Listen.
* Be empathetic.
* Ask questions.
* Provide support.

# —

# Reg D: Convenient Withdrawals

Places restrictions on the timing and number of withdrawals from certain types of accounts. Frontline employees need to be able to explain these restrictions to consumers in order to provide the highest level of service.

Imposes reserve requirements on certain deposits and other liabilities of depository institutions solely for the purpose of implementing monetary policy.

Transaction Limits on Savings Deposit Accounts

Reg D places a limit of six “convenient” withdrawals or transfers per month that a depositor can make on savings deposit accounts.

Saving deposit accounts:

* Money market deposit accounts (MMDAs).
* Share accounts at credit unions.
* Passbook savings accounts.
* Statement savings accounts.

Convenient (the depositor can conduct them with very minimal effort) transfers and withdrawals include:

* Preauthorized, automatic transfers.
* Transfers and withdrawals initiated by telephone, facsimile, or computer, and transfers made by check, debit card, or other similar order made by the depositor and payable to third parties.

Standard withdrawals are sometimes referred to as “inconvenient” or less convenient withdrawals because they require more effort of the consumer. They include:

* Withdrawals made by email, messenger, ATM, or in person.
* Withdrawals made by telephone when a check is mailed to the account holder.
* Transfers made by mail, messenger, ATM, in person, or automatically for repaying loans at the same financial institution where the consumer holds the savings deposit account.

Exceeding Convenient Transaction Limits: if a consumer exceeds his or her monthly transaction limits on a savings deposit account, the financial institution may charge a penalty fee. If the consumer continues to exceed the transaction limits on his or her account, the financial institution must either transfer the funds to another type of account or close the account.

# —

# SAR: Responding to the Suspicious Activity

You have the duty to carefully examine the actions of customers.

FAQs

How can I tell if something is suspicious?

Anything you believe is strange or out of the ordinary.

Are they any legal protections for my institution?

Federal law provides protection from civil liability for filing a SAR (safe harbor). Your institution can elect to file a report in good faith even when doing so is not required. It will not be liable under any state or federal statute.

Who can know about a SAR filing?

SARs are considered confidential and may not be revealed to outsiders under threat of civil monetary penalties. The exception is law enforcement agencies; they obviously will need this information when investigating the suspicious activity, so your institution can share SARs with the relevant authorities.

Recognizing Suspicious Activity

Report Known or Suspected Violations: the motives behind suspicious activity are often criminal. The various federal banking regulators and the Treasury Department have enacted rules which require you and your institution to document and report any known or suspected criminal violation:

* Committed or attempted against the institution.
* Conducted through the institution.
* Involving circumvention of reporting requirements in the Bank Secrecy Act (BSA).
* Involving money laundering.

Situations that require a SAR filing:

* Frequent foreign currency transactions for unusual amounts.
* Two customers arriving together and depositing a combined amount of $10,000
* Bribe attempts or threats.
* Frequent wire transfers for unusual amounts..
* Attempt to avoid reporting requirements.
* Frequent transfers of large amounts to money-laundering havens.

New Accounts Reps should beware of:

* Customer’s permanent address outside of the U.S.
* Customer’s telephone number is no longer in service.
* Customer is unwilling to provide personal background information he/she wants to open a bank account.
* Business customer is hesitant to give details about his/her business activities.
* Business customer is hesitant to provide financial statements/documents.

BSA states that you must file a SAR when you suspect a transaction is conducted or attempted by, at, or through an institution involving or totaling $5,000 in funds, and the institution has reason to know or suspect that:

* The transaction involves funds derived from illegal activities or is conducted to launder money.
* The transaction has no business or apparent lawful purpose or isn’t the type of business that the customer is usually involved with.
* The customer’s transaction is designated to evade any requirement of BSA, including CTR rules.
* Suspicious activity aggregating $5,000 or more when a suspect can be identified.
* Suspicious activity aggregating $25,000 or more regardless of knowledge of a suspect.
* Suspicious activity aggregating $5,000 or more that involves potential money laundering or violations of the Bank Secrecy Act.
* But also of an insider: employee, officer, director or agent of the institution.

Commercial Real Estate Fraud

Commercial Real Estate Fraud Analysis and Advisory (by FinCEN): to provide examples of common commercial real estate fraud schemes, and suggests financial institutions use the term “CREF” when completing SAR narratives involving potential commercial real estate fraud.

Non-Bank Residential Mortgage Lenders: also must have anti-money laundering (AML) programs in place and file SARs when they encounter suspicious activity.

Types of Mortgage Loan Fraud

* ***Occupancy fraud:*** to gain more favorable lending rates, borrowers claim that vacation or investment properties will be their primary residences. This fraud also occurs when borrowers apply for loans for a primary residence that other people (e.g. family members) will occupy.
* ***Appraisal fraud:*** this can take the form of either overstating the home value to obtain more money from a sale or cash-out financing, or understanding home values to purchase property at a steep discount.
* ***Income Fraud:*** borrowers overstate income to qualify for larger mortgages or understate income to qualify for hardship concessions.
* ***Employment Fraud:*** this encompasses any misrepresentation of a borrower’s employment status, including identity of employer, length of employment, unemployment status, and whether the borrower is an independent contractor or business owner.
* ***Liability Fraud:*** borrowers try to hide significant financial liabilities such as car loans, other mortgages, or student loans from lenders to make their loan applications more attractive.
* ***Debt Elimination Schemes:*** any scheme that charges borrowers for invalid or illegal documents that claim to invalidate a mortgage or account balances.
* ***Foreclosure Rescue Scams:*** these deceptions attempt to convince distressed homeowners that they can avoid foreclosure by transferring the title of their home to the scammer or making monthly mortgage payments to the scammer rather than the actual mortgage holder.
* ***Identity Theft:*** involves using a SSN card or any other form of government-issued identification so that the thief can assume someone else’s identity in the mortgage loan process.
* ***Home Equity Conversion Mortgage (HECM):*** seniors are targeted in order to coerce them into turning over their titles to scammers in “reverse mortgage” scams.

Red Flags for Mortgage Fraud: FinCEN has identified numerous red flags that lenders need to be alert for. Lenders should pay attention to:

* The submission of invalid documents to cancel mortgage obligations or pay off a loan balance.
* The same notary and/or “authorized representative” preparing, signing, and sending packages of nearly identical debt elimination documents for multiple borrowers.
* The same notary and/or “unauthorized representative” working with an unusually large number of borrowers.
* Falsification of certified checks or cashier’s checks drawn against borrower’s account rather than the account of a financial institution.
* Borrowers who do not reside in a property purchased as a “primary residence”.
* Younger borrowers whose primary purchase mortgage is for a property in a senior citizen residential development.
* When public and personal documents indicate that borrowers reside at a different location than the address listed on the loan application.
* When language is included in a short sale contract that indicates the property could be resold promptly in a possible violation of FHA regulations.
* Low appraisals and non-arm’s length relationships between short sell buyers and sellers.
* The agent of the buyer and/or seller is not licensed.
* Past misrepresentations made by borrowers in previous attempts to secure funding.
* Improper/incomplete file documentation and borrowers reluctant to provide more information or who break promises to do so.
* The resubmission of a rejected loan application with key borrower details changed from an individual to a company/corporation.
* Attempts by borrowers to structure currency deposits/withdrawals or disguise the true value of assets in order to qualify for loan modification programs for distressed borrowers.
* Requests from third parties on behalf of distressed homeowners to pay fees in advance of the homeowners receiving mortgage counseling, foreclosure avoidance, loan modifications, and other services.
* Third parties who may claim to be associated with the U.S. government and whose solicitations of distressed homeowners include mortgage counseling, foreclosure avoidance, loan modifications, or other related services.

Tax Refund Fraud

When completing SARs on suspected tax refund fraud, financial institutions should use the term “tax refund fraud” in the narrative section of the SAR and provide a detailed description of the activity.

Third-Party Payment Processors

Non-bank, or third-party, payment processors provide payment processing services to merchants and other businesses. Typically, they initiate transactions on behalf of merchant clients that do not have a direct relationship with the payment processor’s financial institution. Payment processors use their own deposit accounts at a financial institution to process such transactions and sometimes establish deposit accounts at the financial institution in the names of their merchant clients. It covers:

* Credit card payments.
* Automated Clearing House (ACH) debits.
* Creating and depositing remotely-created checks (RCCs) or “demand drafts”.

Risk Assessment for Third-Party Processors.

They present a risk to the payment system by making it vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions.Their risk profile can vary significantly depending on the composition of their customer base.

Due Diligence for Third-Party Processors.

* ***Due Diligence:*** financial institutions should conduct thorough initial and ongoing due diligence to determine whether external investigation or legal actions are pending against a payment processor or its owners and operators. They should also determine whether payment processors have obtained all necessary state licenses, registrations, and approvals.
* ***Filing a SAR*** - if they know, suspect, or have reason to suspect that a payment processor has:
	+ Conducted a transaction involving funds from illegal activity.
	+ Tried to disguise funds derived from illegal activity.
	+ Tried to engage in transactions designed to evade BSA regulations or that lack a legitimate business or apparent lawful purpose.
* ***The SAR Form:*** 1) Check the appropriate box on the SAR form to indicate the type of suspicious activity. 2) Include the term “Payment Processor” in both the narrative and portion and the subject occupation portions of the SAR.

Medicare Fraud Schemes

* File a SAR and Call the FBI.
* Record Identifying Information: photographs of the person opening the account and anyone who accompanies him/her. If possible, record pictures of their car as well. Maintain copies of the ID or passport if you suspect that these documents might be fraudulent.

Funnel Accounts and Trade-based Money Laundering

Drug cartels have started using funnel accounts and trade-based money laundering (TBML) to move drug profits across country borders.

1. A business owner, who is colluding with the cartel, opens a business account in one state.
2. Members of the cartel start depositing cash from drug deals into the account in different states.
3. The business owner then uses the money to purchase goods and shops those goods to the cartel’s home country.
4. Once the goods are in the new country, they are sold off, and the cartel pockets the proceeds. The money has now been laundered and sent across the border.

Red Flags for Funnel Accounts and TBML:

* Business accounts that receive multiple cash deposits from states where the company does not operate.
* People who make cash deposits into business accounts but do not seem to have knowledge of the business’s purpose or activities.
* Debits on a business account that do not make sense, given the nature of the business (e.g. a produce company writes checks to a textile manufacturer).
* Checks being deposited into an account with different handwriting on the payee and amount lines than the signature lines. This is a sign that the checks were pre-signed and then handed over to the cartel, which then filled out the payee and amounts.

Human Trafficking and Human Smuggling

The red flags include:

* Multiple wire transfers to a common beneficiary located in a region with high migrant populations and/or significant economic/civic turmoil.
* Frequent transfers to or transactions with beneficiaries located on or near the U.S. border.
* Customers receiving wire transfers from countries with high migrant populations, but who are not nationals of those countries.

Signs of victims being economically exploited:

* A business customer that has virtually no payroll or a payroll much lower than expected given the size of the business.
* A business customer making substantial deductions to its employees’ wages.
* A consumer, escorted by a third party, making a large wire transfer that appears to be most or all of his/her salary.
* Frequent payments to online escort services for advertising.
* Frequent transactions by business customers for good, lodging, and transportation to apparently provide sustenance to individuals.
* Payments to employment or recruitment agencies that are not licensed or registered, or that have labor violations.
* Apparently unrelated personal accounts having the same signers or custodians.
* Accounts of foreign workers or students where the employer or employment agency serves as a custodian.

Reporting Human Trafficking and Human Smuggling: make sure to use the term “Advisory Human Smuggling” and/or “Advisory Human Trafficking” in the narrative portion of the SAR. Do not report the potential victim of smuggling or trafficking as the subject of the SAR.

Filling Out and Filing the SAR

Time restrictions: financial institutions are required to file a SAR no later than 30 calendar days after the date they initially detect suspicious activity. Another 30 calendar days may be added to that deadline (for a total of 60 days max) if a suspect is not apparent and the financial institution attempts to determine his/her identity.

Five Simple and Separate Parts

1. Subject Information.
2. Suspicious Activity Information.
3. Financial Institution Where Activity Occurred.
4. Filing Institution Contact Information.
5. Narrative

After your supervisor completes the SAR, it is electronically filed to FinCEN.

The SAR Form

* ***Home Page:*** asks you to indicate whether you are filing an initial, corrected/amended, or continuing activity report.
* ***Subject Information:*** asks for any information you have about the suspects including suspicious activity involving institution employees.
* ***Suspicious Activity Information***: asks for the date/date range of the activity, characterization of the activity and the dollar amount involved.
* ***Financial Institution Where Activity Occurred:*** asks for descriptive details of your institution such as full legal name, address, EIN, and primary regulator. You’re also asked to give any account numbers affected by the activity.
* ***Filing Institution Contact Information:*** asks for the date the report was prepared. The contact person should have specific knowledge of the activity and also any law enforcement agency you contacted.
* ***Narrative:*** it includes space to provide detailed explanation of the suspicious activity (agents rely on your narrative to make investigative decisions). Give a clear, chronological account of the suspicious activity and dollar amount(s) involved. Also describe any changes that are being made to a previously filed report.

Three (3) Points to Keep in Mind

* ***Attachments***: Excel-compatible comma separated value (CSV) file, no more than one megabyte. Explain in the narrative section.
* ***Recordkeeping***: file the SAR and its documentation in a safe place for a period of five years from the date of the report (e.g. spreadsheets of account activities, photocopies of canceled checks and account statements, and surveillance photos)
* ***Confidentiality***: no bank or other financial institution, and no director, officer, employee or agent of any bank or other financial institution, who reports a suspicious transaction under this part, may notify any person involved in the transaction that the transaction has been reported”.