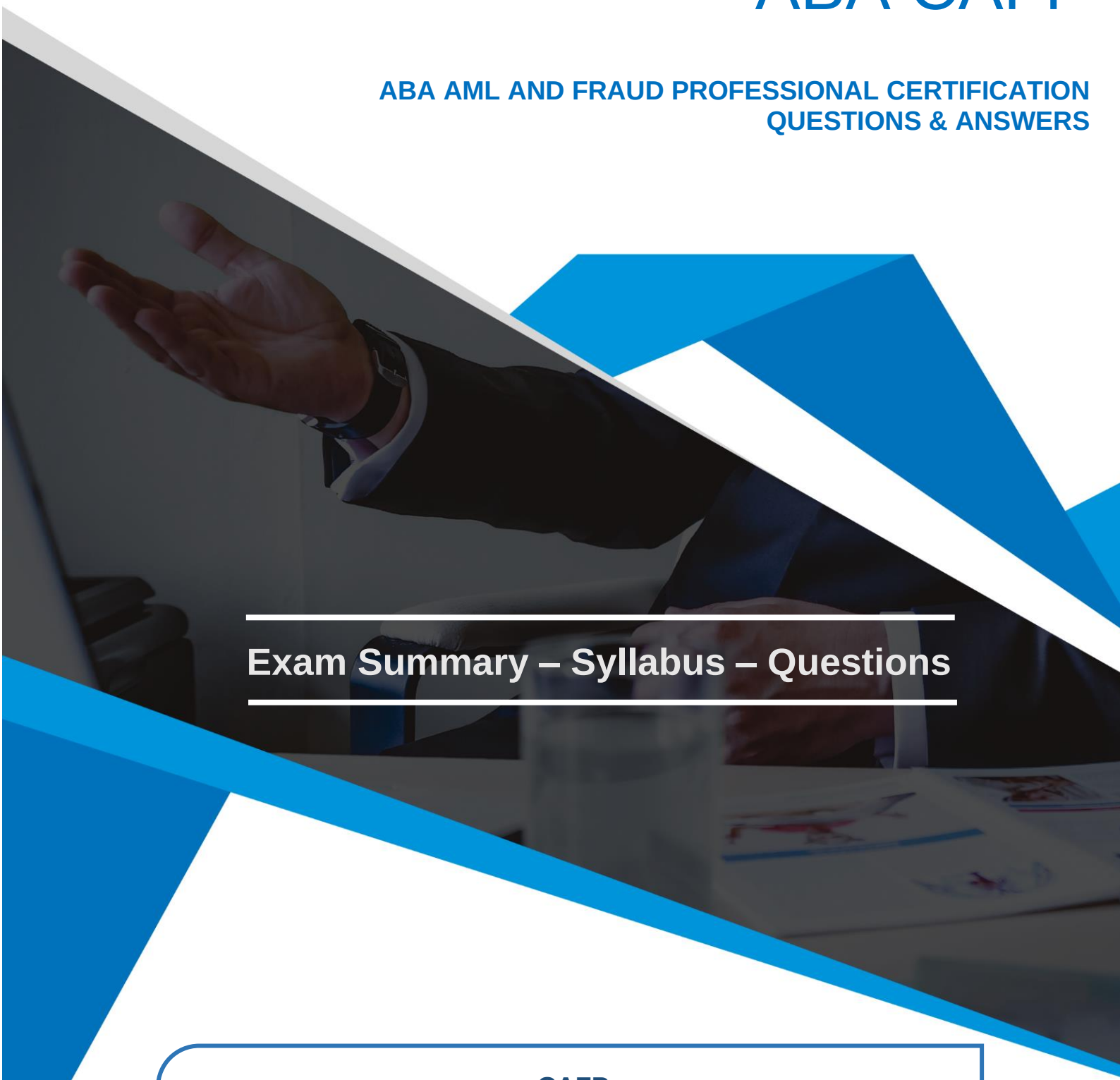
ABA CAFP

ABA AML AND FRAUD PROFESSIONAL CERTIFICATION QUESTIONS & ANSWERS



Exam Summary – Syllabus – Questions

CAFP

ABA Certified AML and Fraud Professional (CAFP)

150 Questions Exam – Pass/Fail Cut Score – Duration of 180 minutes

www.CertFun.com

Table of Contents

Know Your CAFP Certification Well: 2

ABA CAFP AML and Fraud Professional Certification Details: 2

CAFP Syllabus: 3

Assessment - 35% 3

Investigations - 30% 6

Reporting - 17% 8

Remediation - 18% 9

ABA CAFP Sample Questions: 10

Study Guide to Crack ABA AML and Fraud Professional CAFP Exam:..... 12

Know Your CAFP Certification Well:

The CAFP is best suitable for candidates who want to gain knowledge in the ABA Professional Level. Before you start your CAFP preparation you may struggle to get all the crucial AML and Fraud Professional materials like CAFP syllabus, sample questions, study guide.

But don't worry the CAFP PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the CAFP syllabus?
- How many questions are there in the CAFP exam?
- Which Practice test would help me to pass the CAFP exam at the first attempt?

Passing the CAFP exam makes you ABA Certified AML and Fraud Professional (CAFP). Having the AML and Fraud Professional certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ABA CAFP AML and Fraud Professional Certification Details:

Exam Name	ABA Certified AML and Fraud Professional (CAFP)
Exam Code	CAFP
Exam Price	$750 (USD)
Duration	180 mins
Number of Questions	150
Passing Score	Pass/Fail
Schedule Exam	**EXAM APPLICATION**
Sample Questions	**ABA AML and Fraud Professional Sample Questions**
Practice Exam	**ABA CAFP Certification Practice Exam**

CAFP Syllabus:

Topic	Details
Assessment - 35%	
Establish procedures to consistently address regulatory requirements.	Knowledge required: • Risk assessment process - Identification of specific risk categories - Analysis of specific risk categories • Compliance guidance and regulations for a Customer Identification Program (CIP) - CIP notices - Section 311 of the USA PATRIOT Act - Section 326 of the USA PATRIOT Act • Compliance guidance and regulations for customer due diligence (CDD)/enhanced due diligence (EDD) - May 2016 Financial Crimes Enforcement Network (FinCEN) Final Rule CDD/beneficial ownership and FAQs - Federal Financial Institutions Examination Council (FFIEC) special measures • Compliance guidance and regulations for customer risk rating/Know Your Customer (KYC) - FFIEC Appendix K - Customer risk factors to determine overall risk posed to the institution - Procedures for identifying and reporting of suspicious activity • Compliance guidance and regulations for politically exposed persons (PEPs) - FFIEC - FinCEN FAQs and guidance - Fact Sheet for Section 312 of the USA PATRIOT Act Final Regulation and Notice of Proposed Rulemaking • Compliance guidance and regulations for Office of Foreign Assets Control (OFAC) - OFAC regulations for the financial community - OFAC Enforcement Guidelines - OFAC FAQs - FFIEC

Topic	Details
	- "Specially Designated Nationals" (SDN) versus sanctions - Reporting requirements - Record retention - Initial and ongoing screening - Blocking versus rejecting transactions • Fraud guidance and regulations (e.g., identity theft, synthetic, first-party) - Fair and Accurate Credit Transactions Act (FACTA) Red Flags Rule - FFIEC multifactor authentication - Fannie Mae and Freddie Mac requirements - SEC requirements (e.g., Ponzi, pump-and-dump, insider trading) • Cyber guidance - Executive Order 13691 - Executive Order 51117 - Economic Espionage Act of 1996 - FinCEN Advisories FIN-2016-A005, FIN-2016-A003, FIN-2013-A001, FIN-2012-A005, and FIN-2011-A016 - FinCEN Guidance on the Scope of Permissible Information Sharing covered by Section 314(b) Safe Harbor of the USA PATRIOT Act
Evaluate customer risk.	Knowledge required: • Compliance guidance and regulations (e.g., CIP, CDD/EDD, OFAC) - FFIEC - USA PATRIOT Act Sections 312 and 326 - U.S. Treasury Guidance for Financial Institutions - FFIEC Appendix J and Appendix K • Fraud guidance and regulations (e.g., identity theft, synthetic, first-party) - Identity theft (FinCEN advisory, FACTA, Federal Trade Commission [FTC], red flags) - New account fraud (FinCEN advisory, red flags) - First-party fraud (deposit, credit)
Evaluate risk to prevent and detect financial crimes.	Knowledge required:

Topic	Details
	• Relationship risk (e.g., beneficial ownership, account maintenance, vendor, employee, customer) • Geographic risk (e.g., Financial Action Task Force [FATF], State Department, OFAC, U.S. Postal Service, Organisation for Economic Co-operation and Development (OECD), high-intensity drug trafficking area [HIDTA], high-intensity financial crimes areas [HIFCA], Geographic Targeting Orders [GTO]) • Product/service risk (e.g., channels, assessment of risk, fraud solutions) • Cyber risk (e.g., National Institute of Standards and Technology [NIST], SWIFT Customer Security Program [CSP] [self-attestation]) • Transaction risk and fraud types (e.g., counterfeit, lost/stolen, altered, endorsement, account takeover [ATO], e-commerce, unauthorized, scams)
Monitor external sources of information (e.g., negative news, dark web, forums, social media).	Knowledge required: • Common points of purchase (CPP) • Financial Services Information Sharing and Analysis Center (FS-ISAC) • Dark web (compromised data, evolving tactics, threats to an institution) • Open-source intelligence
Participate in internal and external information sharing to gain intelligence.	Knowledge required: • FinCEN advisory (formal collaboration between financial crimes and information security) • FS-ISAC • InfraGard • Section 314(b) of the USA PATRIOT Act • U.S. Secret Service Electronic Crimes Task Force • Department of Homeland Security's Enhanced Cybersecurity Services

Topic	Details
	• Third-party services (FICO, early warning systems [EWS], processors and payment network, roundtable information sharing, BITS)
Analyze an event or alert to determine the next course of action.	Knowledge required: • Anti-money laundering (AML) and fraud scenarios/typologies • Brute force attacks (rainbow table) • Malware • Social engineering (e.g., business email compromise [BEC], distributed denial of service [DDoS], phishing, vishing, spoofing) • Network attacks (Bluejacking, Bluesnarfing, port scanning, device ID) • Jackpotting (hardware/software machine or terminal) • Identification and reporting of suspicious activity
Develop rules and strategies for system alert generation.	Knowledge required: • AML and fraud false-positive rates • AML and fraud detection rates • Control and client impact/customer experience rule • Champion challenger/estimators • Anomaly detection (AML, cyber, fraud) • Model validation • Risk appetite
Investigations - 30%	
Review an activity claim/type in a confirmed case.	Knowledge required: • AML and fraud scenarios/typologies • Cyber-enabled financial crimes typologies • AML/terrorist financing typologies
Identify suspects (known or unknown) and victims in a confirmed case.	Knowledge required: • KYC (e.g., internal information, Sections 314(a) and 314(b) of the USA PATRIOT Act)

Topic	Details
	• Public records • OFAC • Open-source intelligence • Interviewing tactics (e.g., elicitation technique) • Types of law enforcement inquiries (e.g., Section 314(a) of the USA PATRIOT Act, subpoenas)
Determine suspicious activity type and priority level in a confirmed case.	Knowledge required: • Thresholds (e.g., monetary, law enforcement interest, case types) • Recoverability (i.e., transactions and liability) • Types of suspicious activity listed on the suspicious activity report (SAR) form, including “other” • AML and fraud scenarios/typologies
Conduct research by using internal and external sources of intelligence.	Knowledge required: • Internal sources of intelligence - Handwriting comparison - Video surveillance - Telephony (e.g., voice, automated number identification [ANI], device) - Cyber Indicators (e.g., IP address, user agent string, hosting provider, URL, image) - Account relationship/transaction information (e.g., statements, internal communication, account opening documents) • External sources of intelligence - Open-source intelligence (e.g., social media) - Negative news - Screening (e.g., OFAC, external lists) - Section 314(b) of the USA PATRIOT Act
Build the case file, including supporting documentation.	Knowledge required: • How to pull public records • How to analyze account relationship/transaction information (e.g., statements, internal communication, account opening documents) • Time frame requirements (e.g., Regulation E, SAR filing)

Topic	Details
	• Required documents based on activity type • Documentation to support SAR and non-SAR decisioning
Determine the next course of action (e.g., account closure, reporting) in a confirmed case based on the identified risk.	Knowledge required: • Section 314(b) of the USA PATRIOT Act • SAR confidentiality • Customer risk score modification • Financial institution risk appetite • When to elevate the case internally or externally
Reporting - 17%	
Identify appropriate regulatory reporting requirements and file (or assist with filing) initial and ongoing reports (e.g., currency transaction reports [CTRs], SARs, FACTA Red Flags Rule, Report of Foreign Bank and Financial Accounts [FBAR], Bank Secrecy Act Designation of Exempt Person [DOEP]).	Knowledge required: • Thresholds • Time frames • FinCEN e-filing • Appropriate audience for reporting • Record retention requirements • Follow-up reporting • Amendments • Backfiling • Exemptions • Section 314(a) of the USA PATRIOT Act • Section 314(b) of the USA PATRIOT Act • How to report OFAC blocked or rejected customers to the U.S. Treasury
File or assist with filing non-regulatory required reports (e.g., card networks, government sponsored enterprises [GSEs], credit reporting agencies [CRAs]).	Knowledge required: • What to submit to internal or external information sharing partners (indicators of compromise [IOCs]) • How to submit documentation regarding card fraud loss
Respond to law enforcement requests.	Knowledge required: • When a subpoena is required

Topic	Details
	• Parameters of Section 314(a) of the USA PATRIOT Act
Remediation - 18%	
Establish and update controls (e.g., update procedures, tune rules, policy changes).	Knowledge required: • How to identify procedural gaps • How to update procedures to address gaps • How to find guidance and regulatory updates
Manage relationships with customers and intermediaries (e.g., retention or termination).	Knowledge required: • OFAC • Higher risk industries (e.g., marijuana-related businesses [MRBs], money services businesses [MSBs], correspondent banking/SWIFT CSP)
Engage in entity and/or victim remediation (e.g., return money, open new accounts, update third-party agencies, recover funds, charge off).	Knowledge required: • Availability of Funds and Collection of Checks (Regulation CC) • Electronic Funds Act (Regulation E) and error resolution process • Fair Credit Reporting Act (FCRA) • FACTA ID theft remediation • Hold harmless agreement
Educate and train customers, employees, and third parties.	Knowledge required: • Training pillar of Bank Secrecy Act (BSA) • Notice to Customers: A CTR Reference Guide • Identity theft red flags • Emerging typologies

ABA CAFP Sample Questions:

Question: 1

When managing relationships with customers and intermediaries, what is the recommended approach for higher-risk industries?

a) Terminate all relationships with higher-risk industries to eliminate potential risks
b) Ignore regulatory requirements and focus solely on profitability
c) Provide financial incentives to attract more customers from higher-risk industries
d) Conduct enhanced due diligence and monitor transactions closely

Answer: d

Question: 2

Which regulatory body provides compliance guidance for evaluating customer risk?

a) Federal Reserve System (FRS)
b) Financial Crimes Enforcement Network (FinCEN)
c) Federal Financial Institutions Examination Council (FFIEC)
d) Office of Foreign Assets Control (OFAC)

Answer: c

Question: 3

What is the purpose of filing amendments in regulatory reporting?

a) To update the appropriate audience for reporting
b) To submit documentation regarding card fraud loss
c) To backfile reports that were previously missed
d) To rectify errors or provide additional information to the initial report

Answer: d

Question: 4

When establishing and updating controls, what is the purpose of identifying procedural gaps?

a) To comply with regulatory requirements
b) To determine the effectiveness of existing controls
c) To update policies and procedures
d) To identify potential risks and vulnerabilities

Answer: d

Question: 5

Under Regulation CC, what is the maximum hold period for most checks deposited in a transaction account?

a) 1 business day
b) 3 business days
c) 5 business days
d) 7 business days

Answer: b

Question: 6

How can emerging typologies be addressed in the remediation process?

a) By establishing and updating controls
b) By managing relationships with customers and intermediaries
c) By engaging in entity and/or victim remediation
d) By educating and training customers, employees, and third parties

Answer: c

Question: 7

In public records research, what is the purpose of searching professional licensing databases?

a) To find potential investors
b) To identify regulatory compliance issues
c) To access personal medical records
d) To track consumer purchasing behavior

Answer: b

Question: 8

Which organization sets international standards for combating money laundering and terrorist financing?

a) Financial Action Task Force (FATF)
b) State Department
c) Office of Foreign Assets Control (OFAC)
d) U.S. Postal Service

Answer: a

Question: 9

What is a common typology for money laundering through the real estate sector?

a) Using shell companies to purchase properties
b) Structuring cash deposits in small amounts
c) Large-scale cyber attacks on real estate databases
d) Engaging in online auctions for property sales

Answer: a

Question: 10

How can open-source intelligence be useful in investigations?

a) By conducting handwriting comparison
b) By providing public records
c) By monitoring social media and online sources
d) By utilizing the elicitation technique in interviews

Answer: c

Study Guide to Crack ABA AML and Fraud Professional CAFP Exam:

- Getting details of the CAFP syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CAFP exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the ABA provided training for CAFP exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CAFP sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CAFP practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CAFP Certification

Make CertFun.com your best friend during your ABA Certified AML and Fraud Professional (CAFP) exam preparation. We provide authentic practice tests for the CAFP exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CAFP exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CAFP exam.

Start Online Practice of CAFP Exam by Visiting URL

https://www.certfun.com/aba/cafp-aba-aml-and-fraud-professional