ACAMS

CERTIFIED AML FINTECH COMPLIANCE ASSOCIATE (CAFCA)

CERTIFIED
CAFCA™
AML FINTECH COMPLIANCE ASSOCIATE

FinTechs make change happen fast. And, growth can come even faster.

For FinTechs, understanding and mitigating financial crime risk is essential for sustaining growth. Investors, customers, global regulators and financial institutions that provide banking services all expect FinTechs to have a risk management plan in place, and a properly trained workforce.

This new associate level certification enables individuals to demonstrate, and your organization to provide evidence of, financial crime prevention preparedness – designed specifically for your unique context.

What is CAFCA?

CAFCA (Certified AML FinTech Compliance Associate) is a qualification for FinTech professionals, developed by FinTech professionals, and certified by ACAMS. The CAFCA program consists of an 8-hour digital course, and a proctored 90-minute exam.

CAFCA covers:

- **Governance, Guidance, and Regulation**
- **Due Diligence Across Customer Types**
- **Payment Screening and Transaction Monitoring**
- **Investigations, Inquiries, and Reporting**
- **Scaling Anti-Financial Crime Strategies**

The course content has been developed in partnership with FINTRAIL, a specialist FinTech and RegTech consultancy, supporting a global portfolio of rapidly scaling and established FinTech companies, and advisor to leading RegTech firms.

Why was CAFCA created?

Financial crime prevention for FinTechs is different – this program recognizes and responds to that.

CAFCA is designed to upskill and empower the teams you rely on to protect your organization, by ensuring they understand core compliance principles, functions, and risks. A fully certified team also demonstrates that your business takes financial crime risks seriously.

Who is the CAFCA Certification for?

This program is relevant for:

- Small start-ups, with staff in hybrid roles that include AML tasks
- Mid-sized FinTechs transitioning to a more structured AML program
- Large FinTechs with dedicated compliance teams

Companies that would benefit from having CAFCA certified employees include:

- Any FinTech experiencing or preparing for a period of rapid growth
- Payment Service Providers (PSPs)
- Electronic money providers and digital wallets, including pre-paid cards
- Banking as a Service (BaaS) providers
- Neo-Banks, challenger banks, and traditional banks creating new digital products
- Banks accepting FinTechs as customers
- Consultancies managing the outsourced work of FinTechs
- Crowdfunding and peer-to-peer lending organizations
- InsureTech companies
- Investment and wealth management technology companies
- Cryptocurrency exchanges and wallet providers (as relates to cash transfer and exchange aspects, not to blockchain technology)
- Organizations seeking to expand financial inclusion by supporting the “un-banked” in high-risk areas

How to get certified

1. Join ACAMS

ACAMS membership is required to apply and maintain your certification.

2. Prepare & Apply

Complete your learning path and submit your application to schedule the exam.

3. Schedule & Pass

Once your application is approved, you’ll receive instructions by email to schedule your exam. Pass the exam to earn your certification and maintain it through ongoing membership and education.

Certification Package and Pricing

For group discounts, request a consultation.

The certification package includes:

- Study guide (PDF)
- Flashcards
- Online study materials (post-assessment)
- Practice exam
- Certification exam

US$1,045

ACAMS

CERTIFIED CAFCA AML FINTECH COMPLIANCE ASSOCIATE

What Workforce Competencies are tested by the CAFCA Exam?

1. Governance, Guidance, and Regulation (20%)

1.1. Definition and types of FinTechs (e.g., PSPs, digital wallets, cryptocurrency exchanges) and features of FinTechs that make them vulnerable to financial crime

1.2. Types of financial crime (e.g., money laundering, fraud (both first-party and third-party), sanctions, terrorist financing) and predicate crimes (e.g., bribery, tax evasion)

1.3. Regulatory principles that apply to different FinTech business models (e.g., registration, licensing, banking charters) and differing AML requirements, including the purpose and guidance around sandbox usage

1.4. Risk management framework (lines of defense, policies and procedures, principles of assurance and quality control, responsible party (e.g., MLRO)

1.5. Best practices in handling sensitive/private information, including definitions of PII and SPII, privacy laws (e.g., GDPR, CCPA), reporting cybersecurity breaches/ incidents, the consequences of inappropriate data handling

1.6. Definitions and key components of riskbased approach, risk assessment, and risk appetite including their purpose and when to review and update

1.7. Types of sources available to reference to guide the development of processes

1.8. How FinTechs are risk-categorized by more traditional institutions and how to maintain the relationships (onboarding and ongoing, de-risking)

1.9. Control framework to mitigate internal threat

1.10. Types of risk (e.g., reputational, business, operational, financial, regulatory)

2. Due Diligence Across Customer Types (20%)

2.1. CIP/KYC/eKYC/CDD/EDD processes, including definitions, core activities, and best practices (e.g., understanding account purpose and ownership, setting baseline activity), and how risk-based approach is applied

2.2. Identification verification/digital identification verification principles (e.g., matching data points) including expected documents/ document quality

2.3. Data sources to verify customer information (e.g., online searching, open-source, private and public third- party data providers, fraud) and how to determine the reliability of these sources

2.4. Data that can be used to verify customer information (e.g., IP address, GPS coordinates, MAC addresses, application completion time, copy/paste use)

2.5. Principles and purpose of screening for sanctions (e.g., information that indicates a sanction concern, how to select the appropriate sanctions list), PEPs (the risks PEPs pose, foreign v. domestic PEPs), and fraudsters

2.6. Risk ratings, including the types of risk factors (e.g., types of customers), the information to include in the risk rating, and how to access this information (e.g., internal and external data sources), how risk algorithms work

2.7. Red flags for fraudulent activity in onboarding (e.g., spoofing, identity theft, counterfeit documentation)

3. Payment Screening and Transaction Monitoring (25%)

3.1. Purpose of transaction monitoring

3.2. Purpose of and red flags in screening payments (e.g., sanctions and fraud) and the decisions to be made when screening

3.3. Red flags of financial crimes in transaction monitoring (e.g., layering funds, integrating funds) and characteristics of suspicious transactions

3.4. Common payment transaction methods, including cryptocurrency and other high-risk transactions (e.g., aggregation)

3.5. Investigatory process for alerts (e.g., determining unusual/suspicious activity, determining escalation)

3.6. Best practices in creating an audit trail (i.e., documentation) for all suspicious activities

3.7. Types of transactions for FinTechs and associated risks (e.g., reversible v. non-reversible, convertible v. non-convertible, fund integrity, cryptocurrency (privacy coin)

3.8. Transaction monitoring systems and software, including how thresholds are set and adjusted, model validation, rule-based (e.g., pattern recognition) v. machine learning

3.9. Best practices for communicating transaction monitoring trends/results, including KPIs, OKRs, and other statistics

4. Investigations, Inquiries, and Reporting (20%)

4.1. Appropriate customer communication (e.g., what questions can be asked of the customer, what information can be disclosed during investigations and offboarding)

4.2. How to review KYC information, transactions, open-source research, documentation to inform the investigation

4.3. Analytical principles in an investigation (e.g., confirmation bias)

4.4. SARs/STRs, including definitions, when and where they are required, why they are important, and best practices for writing them

4.5. How to work and communicate with third-parties (e.g., law enforcement, banking partners, regulators)

4.6. Types of law enforcement requests (e.g., information, court order), both domestic and international

4.7. How to communicate with customers for financial crime risk v. violation of company policy

4.8. How banking partners' terms of service relate to FinTech's terms

5. Scaling Anti-Financial Crime Strategies (15%)

5.1. How to assess new products/additional features and associated potential risks and necessary controls (e.g., elements of new products that present particular risks (e.g., products moving from domestic to international, offering new types of accounts, changing payment processes, adding distribution channels))

5.2. Importance of reviewing and updating the risk assessment as a part of scaling

5.3. Types of changes that should lead to a financial crime assessment review

5.4. Methods and rules of record retention and data storage

5.5. Considerations of outsourcing controls (e.g., surge capacity, RegTechs, independent testing of compliance framework)