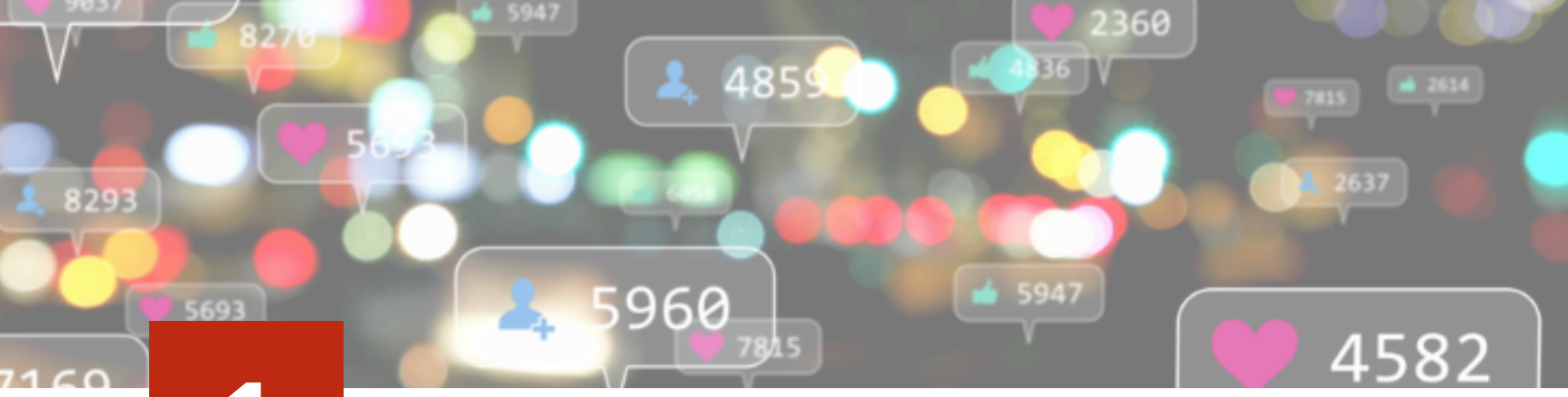
FATF

FINANCIAL ACTION TASK FORCE

Detecting and Disrupting Terrorist Financing Activity

THROUGH SOCIAL MEDIA, INSTANT MESSAGING APPLICATIONS AND STREAMING PLATFORMS

June 2026



1 Introduction

01. Countering the financing of terrorism (CFT) continues to be a priority for the Financial Action Task Force (FATF), given the serious ongoing and evolving threats posed by terrorist organisations and individuals around the world. These threats range from small cells to large-networked organisations operating across borders and/or possessing territorial control capabilities.

02. Terrorists have demonstrated their persistent ability to abuse the international financial system to raise, move, store and spend funds to support their financial and operational needs. The financing methods used by terrorist actors can vary considerably, in part depending on their access to emerging technologies, digital platforms, and social media, instant messaging applications and streaming platforms (SMSPs), and on their ability to adapt their financing methods to the new technology available.

03. Building on the FATF's Comprehensive Update on Terrorist Financing Risks (2025), FATF members decided to deepen their knowledge on how SMSPs can be abused for TF purposes. This document raises public awareness among stakeholders of the issues identified by the FATF to support operational authorities in detecting, disrupting, investigating, and prosecuting TF activity if it occurs on SMSPs.

SMSP ecosystem and exposure to TF risk

The SMSP ecosystem extends from mainstream social networks to encrypted messaging apps and is designed for accessibility and scalability. The core functionalities of these networks and apps include instant messaging, multimedia sharing, group creation, and, **increasingly, the availability of payment functionalities embedded in the user interface or enabled through third-party business partners.**

SMSPs have **evolved from purely communication tools into more complex digital ecosystems** integrating financial services and revenue streams. SMSPs and large technology or telecommunications providers generally do not provide payment services directly but instead operate as platforms through which regulated or unregulated third-party payment service providers (PSPs) integrate and offer such services. AML/CFT obligations apply to these PSPs depending on the materiality and nature of their activities. Ongoing technological developments require continuous monitoring, as successive generations of payment systems become more deeply embedded within platform interfaces, potentially blurring traditional regulatory boundaries.

The risk exposure of SMSPs primarily concerns their potential use for the raising and movement of funds, which differs from their role in communication and content sharing. As the SMSP ecosystem expands, this risk is expected to grow.

Jurisdictions contributing to this work highlighted almost an equal distribution of terrorist threats abusing SMSPs for financing purposes: individual terrorists, including foreign terrorist fighters and small cells (30%), ethnically or racially motivated terrorist organisations and individuals (26%), large-networked organisations relying on regional and domestic affiliates (25%) and non-affiliated regional and domestic terrorist groups (19%) were highlighted as abusing this ecosystem.

In addition, less than 30% of jurisdictions that contributed to this report cover TF risks through SMSPs in their national risk assessments and 38% of those identified such risk in their countries as moderate. At the same time, in conflict zone areas and/or areas dealing with active terrorism threats, the risk of SMSPs' abuse for TF purposes is generally reported as high or very high.

SMSPs impact the TF risk landscape due to their fundamental characteristics: (i) their transnational access and reach; (ii) large userbase through increased adoption; (iii) the speed of information collection and exchange; and (iv) the use of filtering systems including algorithms to recommend and promote user-based content. Coupled with anonymity-enhancing technologies, these characteristics enable organised criminal syndicates and terrorist groups to operate transnationally and enhance the effectiveness of their illicit schemes.

Differences in the use of SMSPs for terrorism and TF purposes

Distinguishing between the use of SMSPs for terrorism-related activities and for TF purposes remains a challenge for competent authorities, particularly given the overlap between communication, propaganda, recruitment and financial activities occurring through these platforms. In addition, most enforcement and compliance mechanisms implemented by SMSPs are primarily focused on the detection and removal of terrorist and extremist content, while enforcement mechanisms to identify and disrupt TF activity are still developing.

Terrorist groups generally exploit social media's reach and viral dynamics, and encrypted messaging applications can further support operational coordination by enabling communication, sharing, gaining influence, online fundraising and for logistics for donations rather than direct financial transactions.

The use of SMSPs for TF purposes involves exploiting the platforms' financial functionalities and informal value transfer mechanisms. Messaging apps with integrated payment systems, such as VA wallets or features, enable peer-to-peer (P2P) transfers to bypass the applicable customer due diligence (CDD) requirements.

The table below briefly describes the main differences in the nature of abuse of SMSPs:

	Abuse for terrorism purposes	Abuse for TF purposes
Primary objective	Spread propaganda, recruit members and coordinate operations (terrorist acts)	Raise, move and conceal funds to support terrorist organisations' activities
Main activities	Disseminating terrorist activity-related content, encrypted operational planning, networking	Crowdfunding, P2P transfers, use of integrated payment systems
Key features exploited	Viral content sharing, anonymity, encryption	Weak CDD, cross-border payment options, virtual assets (VAs) integration
Nature of abuse	Ideological and logistical	Financial and transactional
Detection challenge	Monitoring encrypted communications and content moderation	Tracking small, frequent transactions and informal value transfers

2 Key trends and typologies

Impact on the TF risk landscape and response needed

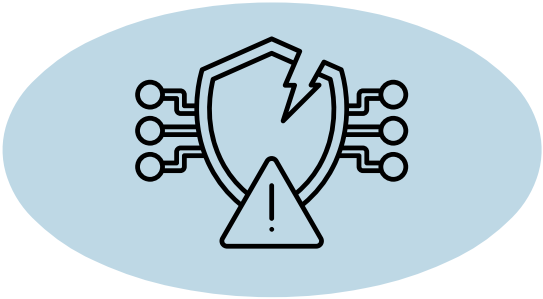
- **Blurring of regulatory responsibilities**: As SMSPs integrate financial functionalities through their interfaces or third-party partners, clearer frameworks are needed to determine which services fall under AML/CFT obligations and by which entity.
- **Increased operational complexity and opacity**: Advanced technologies enable faster, more layered, and harder-to-detect TF activities, requiring continuous adaptation of risk assessments and typologies.
- **Emerging vulnerabilities in monetisation models**: New revenue streams (e.g. livestreaming, subscriptions, digital tipping) create novel TF pathways that require targeted oversight.
- **Rapid technological evolution is reshaping TF risks**: New features such as AI driven content, encrypted communications, VAs, Decentralised Finance (DeFi), and embedded payment tools are continuously expanding the ways SMSPs can be exploited, and competent authorities need to be up to date in understanding potential risks if abused.

Identified typologies of SMSPs for TF purposes as follows:

Typology	Description
Humanitarian-fronted crowdfunding & fake charities	Use of social media to solicit funds through fraudulent humanitarian or charitable appeals, often targeting diasporas and relying on micro-donations and exploiting user trust and platform reach to disguise the true intent and reduce scrutiny. Front organisations or pages collect funds that are diverted to terrorist purposes, sometimes alongside terrorism-related content.
Multi-platform and SMSPs multi modal usage	Fundraising begins on mainstream SMSPs and shifts to encrypted messaging or private groups for coordination and payment instructions, reducing visibility and enabling secure exchange of financial details. Payment details (accounts, wallets, coded instructions) are exchanged directly between trusted members.
Off-platform and diversified payment methods	Redirection to external payment channels (bank transfers, third-party payment systems providers, VAs, cash collection, prepaid cards), often combined with informal transfer systems (e.g. hawala) to obscure transaction trails. Online donations are converted into cash or value via hawala, mobile money, cash pick-ups, prepaid cards, airtime credits or digital vouchers to obscure transaction trails.
Exploitation of platforms' features and amplification tools	Use of paid advertisements or boosted content, bots, fake or compromised accounts, and creator-economy features (e.g. live streaming, tipping) to increase reach, legitimacy, and revenue generation.
VA fundraising and in-app wallets	Use of VA wallets (including in-platform wallets) and QR codes for cross-border transfers, often with rotating addresses and limited CDD, increasing anonymity and reducing traceability.
Camouflage, coded communication & evasion techniques	Terrorist actors employ coded wording, emojis, numbers, and insider references to signal fundraising activities while avoiding detection, often framing requests as humanitarian, religious, or community support. Use of coded language, symbols, slogans, and humanitarian or religious narratives to conceal intent, evade detection, and strengthen in group identity—often combined with encrypted or ephemeral communications.
Disguised commercial activity (layering)	Fundraising is masked as online sales, marketplace listings, or ticketed events, allowing proceeds to be mixed with legitimate-looking transactions.
In-kind procurement	Funds raised online are used directly to purchase goods (e.g. food, fuel, equipment or supplies) delivered locally, bypassing formal financial channels.

Typology	Description
Extortion and kidnapping proceeds	Messaging applications are used to communicate demands, coordinate payments and move proceeds from extortion or kidnapping through digital or informal channels.
Targeting of youth and vulnerable cohorts	Terrorist actors deliberately target young and socially vulnerable individuals through emotionally driven, humanitarian-framed appeals on platforms popular with these groups, exploiting empathy, identity, and belonging to generate donations and, in some cases, broader radicalisation.
Trust-building and tailored digital engagement for mobilisation	Networks use sustained messaging, peer validation, and tailored content (including local languages, youth-oriented narratives, and AI-enabled amplification across platforms) to build credibility over time, embedding donation requests within trusted communities and progressively converting users into financial supporters or facilitators.
Exploitation of creator economy features for fundraising	Terrorist actors and sympathisers generate revenue through platform monetisation tools—such as live streaming, pooled donations, and engagement-based income—blurring the line between legitimate earnings and funds linked to extremist ecosystems. Content-driven monetisation is characterised as a TF pathway as content is leveraged as a revenue-generating asset, with aggregated payment mechanisms obscuring funding sources and enabling individuals to accumulate and potentially redirect income towards activities related to terrorism.
Abuse of payment systems incorporated into the SMSPs interface	Terrorist actors exploit integrated wallet features to send, receive, and exchange VAs directly within messaging platforms, enabling seamless fundraising and transfers with reduced reliance on external financial systems. The combination of in-app wallets and encrypted communication channels allows threat actors to conduct fundraising campaigns—particularly linked to conflict zones—while obscuring identities, increasing adoption, and challenging detection and disruption efforts.
Use of contextual factors as catalysts for social media fundraising campaigns	Terrorist actors leverage conflicts, humanitarian crises, and political developments to initiate and amplify fundraising campaigns, framing appeals as urgent humanitarian or solidarity efforts to attract broad support. By aligning messages with emotionally resonant events and disseminating them quickly these actors increase legitimacy, expand reach, and accelerate donations before detection or countermeasures can be applied.

- SMSPs are increasingly used as trust-building infrastructures for TF, combining public platforms to amplify fundraising narratives with encrypted messaging apps for coordination, payment sharing, and moving activities into private channels—often relying on small, crowd-sourced donations framed as humanitarian support.
- As platforms expand payment and monetisation features, terrorist actors increasingly exploit these tools to raise, move, and manage funds, leveraging integrated functionalities and encrypted environments to coordinate operations and evade detection.
- These typologies demonstrate a high degree of adaptability, with actors rapidly adjusting their methods in response to platform features, regulatory measures, and geopolitical developments. As a result, typologies observed today will continue to evolve, requiring evolving risk-based responses rather than point-in-time responses.



Status quo under the FATF Standards

3

SMSPs do not currently fall under one of the sectors which are required to be subject to AML/CFT obligations under the FATF Standards and therefore, most national frameworks. **However, their progressive evolution into platform-based ecosystems that integrate or enable access to a range of financial services means that certain activities conducted through or facilitated by SMSPs may fall within the scope of sectors already regulated under the FATF Standards. Functionalities supporting financial intermediation—such as VA wallets and transactions, P2P transfers, in-app payment mechanisms**, marketplaces, creator monetisation tools, and embedded e-commerce may trigger the application of relevant FATF Recommendations depending on the nature, scale, and control exercised by the SMSP or associated third-party providers.

For this purpose, it is important to distinguish between situations in which the SMSP provider operates as a neutral platform enabling third-party service providers to offer financial services, and those in which the provider itself performs functions that fall within the definition of a financial institution (FI) or virtual asset service provider (VASP). Where an SMSP merely provides the technical infrastructure or user interface through which licensed or otherwise regulated third-party providers deliver payment or VA services, AML/CFT responsibilities may primarily attach to those third parties. Subject to the degree of control, influence, or benefit retained by the SMSP, there may be some secondary or other obligations on the SMSP. Conversely, where the SMSP directly offers, controls, or materially influences financial services through its interface (such as custody, transfer, exchange, or facilitation of funds or VAs), it may itself fall within the definition of a regulated FI or VASP), and corresponding AML/CFT obligations may apply directly to the SMSP on a functional basis.

Main function	Purpose
In-app purchase	Enables users to buy virtual goods, premium features, or content directly within the platform. Acts as an entry point for monetisation and microtransactions. Common in gaming, creator platforms, and social apps (e.g., buying stickers, virtual gifts, or ad-free experiences).
P2P	Allows users to send money directly to other users within the app. This can refer to transfers between unhosted wallets or just a payment between individuals intermediated by one or more PSP.
Merchant payments	Supports transactions between businesses and consumers through integrated payment gateways. Used for social commerce (e.g., buying products from influencers or brands within the app).
Payouts to users/creators	Platforms pay creators or influencers for monetised content, ads, or virtual gifts. These financial mechanisms are critical for sustaining creator economies and incentivising engagement and may involve direct bank transfers or wallet-based payouts.
Integration with third-party VA wallets	Provides a stored-value account within the platform for holding funds. It enables quick payments for services, tipping creators, or purchasing goods. Often linked to loyalty programmes or VAs.
Integration with banking services	Extends beyond payments to offer banking-like features (e.g., loans, savings, credit). Positions platforms as fintech players, reducing reliance on traditional banks.
VA payments	Enables transactions using VAs or tokenised assets. Adds cross-border payment capability and appeals to tech-savvy users.
Integration of VA wallets	VA platforms integrated into the instant messaging application interface offering dual wallet experience: custodial VA wallet for the general audience and a self-custodial wallet.

Note: The information provided in the above table is based on jurisdictions' submissions to the project and open source research. Business models continuously change and this table is provided for illustrative purposes only and is not exhaustive or authoritative on the activities performed by companies.

The table above aids understanding of how financial services are delivered—either integrated within the platform or via redirection—and identifies the payment systems within the SMSP ecosystem that can fall under the definition of FIs or VASPs from a functional perspective.

SMSPs facilitate financial flows through a range of business models and monetisation mechanisms that combine communication services with payment functionalities and other forms of economic activity. Understanding these models is important for competent authorities, as they can indicate how funds are generated, transferred, or integrated within the platform ecosystem.

SMSP's business model	Monetisation characteristics
Advertising-driven revenue	Platforms monetise user attention by delivering highly targeted ads based on behavior and engagement. Revenue increases with user activity, while creators may receive payouts linked to performance metrics (views, ads, subscribers).
Data-power personalisation and analytics	User data is leveraged to improve services and optimise advertising effectiveness. Platforms monetise insights by offering analytics tools and audience data to creators, advertisers, and businesses.
Subscription/ monthly fee services	Users pay recurring fees for premium features such as ad-free experiences or advanced tools. These subscriptions often include exclusive content, enhanced functionality, or business upgrades.
In-app purchases	Revenue is generated through the sale of digital goods and feature upgrades within the platform. Users can enhance their experience by purchasing virtual items, add-ons, or premium functionalities.
E-commerce integration or social commerce	Shopping is embedded directly into the platform, allowing seamless browsing and purchasing. SMSPs earn through transaction fees, commissions, and partnerships, often via creator-led sales or live shopping.
Creator economy monetisation or affiliate marketing	Platforms enable creators to earn via subscriptions, tips, ads, digital products, and virtual gifts. Some use proprietary tokens purchasable with fiat money, which creators can later convert into cash.
Application Programming Interface (API) and enterprises services	Platforms offer paid tools for businesses, including automation, messaging, analytics, and integration. Revenue comes from charging for high-volume usage, advanced features, and enterprise-level services.
Integrated platform systems and cross-platforms monetisation	Companies link multiple apps and services to maximise user engagement and cross-selling opportunities. Revenue is diversified through bundled ads, subscriptions, and tools across interconnected ecosystems.
Tip functions	Users can send voluntary payments to creators via linked third-party payment services. The platform facilitates visibility and access but does not process payments itself, relying on external providers.

Note: The information provided in the above table is based on jurisdictions' submissions to the project, private sector and academia targeted consultation and open-source research. Business models continuously change and this table is provided for illustrative purposes only and not exhaustive or authoritative on the activities performed by companies.

Where these activities are conducted by an SMSP, it is important for competent authorities to assess whether the SMSP could, in practice, be acting as an FI or a VASP under the FATF Standards. Where such functions are identified, the corresponding AML/CFT obligations shall apply. As noted in Recommendation 31, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures to obtain records held by FIs, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence. This is particularly relevant when SMSPs hold, or process data linked to financial activities normally carried out by regulated sectors, as it can open a series of opportunities to track the financial flows occurring within the features of these platforms and can contribute to understanding the connection nodes of terrorist organisations' financing operations. When combined with publicly available content posted on the platform, such information can provide key evidentiary elements to connect an account or user to a terrorist organisation or related financial activity.

SMSPs are increasingly exposed to financial flows due to the integration of payment mechanisms within their platforms or through user-generated content that includes payment and transfer links.

4 Operational response needs and Private Sector

Operational response needs

No single jurisdiction or authority can address TF risks through SMSPs in isolation. Monitoring, managing, and mitigating these risks requires a coordinated, multi-layered response across domestic authorities, public–private partnerships (PPPs), and international cooperation, supported by frameworks that can adapt to rapidly evolving technologies and threat actors.

Effective detection of TF activity through SMSPs depends on:

1. **Clear risk indicators and triggers** to help operational authorities in identifying the underlying criminal activity.
2. **Coordinated and multi-layered approach to identify, investigate and prosecute** TF through SMSPs (e.g. FIUs, law enforcement, prosecutors, supervisors).
3. **Robust investigative approaches**, including open-source intelligence (OSINT), network analysis, and advanced monitoring techniques.
4. **Engagement between FIUs and regulated entities** (e.g. FIs, VASPs, DNFBPs) to access financial intelligence and ensure application of CDD and transaction monitoring when applicable.
5. Establishment of **bilateral communications channels with SMSPs** to streamline information sharing on specific cases and emerging trends, including through public–private partnerships.
6. **Timely information-sharing and data preservation mechanisms**.

These measures should be in accordance with the applicable legal frameworks, respecting international humanitarian law and data protection and privacy.

Role of the private sector

The private sector plays a critical role by providing data, technological capabilities, and early detection mechanisms to identify and help disrupt TF activity through SMSPs. The private sector has the capacity and resources to develop advanced detection and prevention tools, including AI-driven solutions to identify terrorism and TF-related activity at early stages acting as the first line of defence. As such, they have the capacity to suspend users' transactions and communications on reasonable suspicion for terrorism and TF related content. These actors host and can provide critical data, visibility, and enforcement capabilities that complement and strengthen authorities' ability to detect and disrupt TF activity. SMSPs can provide early detection signals and operational insights that enable faster action by competent authorities. This can be facilitated by authorities providing SMSPs with a clear description of the contextual factors on the case, the offence under investigation, the relevant identifiers on the activity and/or suspects under investigations.

A win–win approach through public–private partnerships (PPPs):

Strengthening cooperation between the tech industry, SMSPs, FIs, PSPs, VASPs, and competent authorities creates mutual benefits. As the industry gains deeper insight into TF trends, it can design more effective algorithms and safeguards to prevent misuse while protecting and enhancing legitimate business. At the same time, law enforcement authorities (LEAs) benefit from faster access to high-quality signals and can respond more rapidly to suspicious activity identified by the private sector.

Stronger PPPs are essential to improving the understanding of emerging TF risks and typologies associated with SMSPs. Continued cooperation between SMSPs, regulated financial and CFT entities, and competent authorities will remain fundamental to developing coordinated and effective mitigation measures. Key focus areas include information sharing on emerging trends and best practices for submitting and handling information requests, enabling more efficient and coordinated disruption of TF activity.

Key message: Effective collaboration allows better risk mitigation while supporting legitimate business operations.

Recommendations 5

The challenge for the global community is not innovation itself but ensuring that new financial solutions are developed and deployed in a manner that is resilient to abuse, grounded in strong AML/CFT safeguards when applicable, and aligned with a risk-based approach. Addressing the misuse of SMSPs for terrorism and TF purposes requires jurisdictions to break down institutional silos and strengthen both domestic interagency co-ordination, and international cooperation among the competent authorities involved in the detection, disruption, investigation, and prosecution of TF activity. Proactive engagement with SMSPs will also help develop a shared understanding of potential risks and emerging trends as technology continues to evolve. This effort should involve not only operational authorities, but also policymakers and legal experts to ensure that responses remain effective.

Strengthen structured dialogue between competent authorities and the private sector

Including SMSPs, financial institutions (FIs), and VASPs—recognising their complementary roles in identifying and detecting terrorist and TF-related activity, with SMSPs providing visibility over observed online behaviours and financial service providers tracing the raising and movement of funds.

When possible, establish legal frameworks for timely, secure data exchange between SMSPs, FIs, VASPs and competent authorities, in line with data protection and privacy rules. Competent authorities are encouraged to provide clear, case-specific context to support targeted requests, while SMSPs are encouraged—within a safe and predictable framework—to share insights on emerging risks and suspicious activity trends identified through their enforcement efforts.

Enable effective information sharing and deepen PPPs

Clarify regulatory scope

Continue to develop a better understanding of which SMSP functionalities fall under FATF Standards and identify where AML/CFT obligations shall apply.

Continuously assess TF risks associated with emerging technologies by incorporating private sector expertise in risk assessments, enhancing insight into evolving trends and typologies (i.e. AI, encrypted communications, VAs, Decentralised Finance (DeFi), embedded payments).

Strengthen understanding of risk

Enhance inter-agency coordination

Improve collaboration across FIUs, supervisors, LEAs (including CT/CFT, cyber, units) and intelligence bodies.

Strengthen capabilities to connect financial transactions with online behaviour, content, and networks.

Link financial and digital intelligence

Strengthen international cooperation

Improve cross-border access to electronic evidence and streamline the use of legal cooperation mechanisms.

Provide specialised training and tools to detect and investigate TF involving digital ecosystems.

Build operational capacity

Develop targeted indicators

Expand typologies and red flags specific to SMSP abuse (e.g. coded language, QR codes, monetisation tools).

Assess risks of donations, livestreaming, subscriptions, advertising revenue, and crowdfunding functionalities when applicable.

Increase understanding of monetisation features

www.fatf-gafi.org