Beyond Transactions: Addressing the Pathways to Harm in Modern Illicit Finance -

Submission to the Parliamentary Joint Committee on Intelligence and Security review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026

Review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026

Beyond Transactions: Addressing the Pathways to Harm in Modern Illicit Finance

Away from Keyboard Inc.
Shop 4, 115 Anzac Ave., Seymour VIC 3660
[redacted]
www.afk.org.au

Beyond Transactions: Addressing the Pathways to Harm in Modern Illicit Finance -

Submission to the Parliamentary Joint Committee on Intelligence and Security review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026

Table of Contents

Beyond Transactions: Addressing the Pathways to Harm in Modern Illicit Finance -

Submission to the Parliamentary Joint Committee on Intelligence and Security review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026

Executive Summary

I welcome the opportunity to contribute to the Parliamentary Joint Committee on Intelligence and Security review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026.

This submission supports the intent of the Bill and the broader objective of ensuring Australia's anti-money laundering and counter-terrorism financing framework remains responsive to a rapidly changing threat environment.

Illicit finance is no longer confined to traditional models of criminal activity followed by concealment of proceeds. It now sits within a broader ecosystem shaped by emerging technologies, real-time financial infrastructure, and increasingly sophisticated forms of deception and coercion. Criminal networks are more adaptive, more distributed, and less reliant on physical or institutional constraints. They can generate, move, and obscure value at a speed and scale that places sustained pressure on existing safeguards.

This shift has practical consequences. Systems designed to detect suspicious transactions are increasingly encountering harm only after it has occurred. The point at which money becomes visible to regulatory systems is often the final stage of a longer chain of exploitation involving manipulated trust, identity misuse, targeted vulnerability, and digitally enabled coercion.

In this context, the proposed power enabling AUSTRAC to restrict or prohibit high-risk mechanisms used to provide designated services is both necessary and proportionate. Where systems are demonstrably facilitating serious harm, the capacity to intervene early is essential.

At the same time, strengthening regulatory authority alone will not be sufficient. The operating environment in which illicit finance occurs has changed in three important ways.

The cost of deception has fallen, while its scale and reach have increased. Emerging technologies enable convincing impersonation, targeted manipulation, and automated outreach at volumes previously impossible.

The speed of harm has increased, while response pathways remain comparatively slower and more fragmented. This creates a consistent gap between the pace of exploitation and the pace of intervention.

Beyond Transactions: Addressing the Pathways to Harm in Modern Illicit Finance -

Submission to the Parliamentary Joint Committee on Intelligence and Security review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026

Vulnerability is increasingly targeted with precision. Many forms of contemporary fraud rely not on technical compromise, but on identifying individuals and communities more likely to trust, respond, or comply under pressure.

Taken together, these dynamics mean that illicit finance is increasingly the downstream effect of upstream exploitation systems.

For this reason, effective reform should not focus only on the movement of illicit funds after harm has occurred. It should also consider how those funds are generated and how earlier intervention can be achieved across systems that are currently operating in isolation.

The strongest national response will combine regulatory authority with faster operational pathways, improved frontline recognition, better information flow between institutions, and a clearer understanding of how modern harm is produced.

Introduction

I write as the Founder and Chief Executive Officer of Away From Keyboard (AFK) Inc., an Australian charity focused on digital safety, prevention of technology-enabled harm, and safer system design.

My work sits at the intersection of emerging technologies, public safety, and human rights due diligence. I contribute across policy, advocacy, and standards development, with a focus on how digital systems shape real-world risk, access to safety, and institutional trust. This includes examining how technologies designed for efficiency and scale can also create unintended pathways to exploitation when safeguards are not embedded early.

In addition to leading AFK, I serve as an Adviser to the National Council of Women Victoria across Human Rights and ICT portfolios, and as Co-Lead of Digital Safety Futures for Soroptimist International Australia. I also contribute to international standards development as Co-Vice-Chair of the IEEE Industry Connections Activity focused on User-Centred Principles for Artificial Intelligence Used in Evaluating Family Violence.

My work extends to international engagement, including participation in the United Nations and Asia-Pacific processes examining digital safety, access to justice, and the human rights impacts of emerging technologies. Through these contributions, I have engaged in discussions on technology-facilitated harm, governance gaps, and the need for prevention-focused approaches that can operate at the speed and scale of modern risk.

Beyond Transactions: Addressing the Pathways to Harm in Modern Illicit Finance -

Submission to the Parliamentary Joint Committee on Intelligence and Security review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026

I am also an active member of professional networks focused on cybersecurity, artificial intelligence, and ethical technology governance, including the Australian Information Security Association, the Australian and New Zealand Society of Criminology, and international initiatives examining safe and ethical AI. These engagements support ongoing insight into how risk is evolving across technical, regulatory, and social domains.

As a community-based organisation operating in regional Australia, AFK brings a perspective informed by both local experience and global engagement. This includes direct insight into how digital harms affect individuals, families, schools, and services, particularly in contexts where access to specialist support and justice pathways may be more limited.

Across this work, a consistent pattern has emerged. Increasingly, the most significant risks are not occurring within a single system, but across multiple connected systems that were not designed to operate together. Harm is often generated upstream, through deception, coercion, and targeted vulnerability, before it becomes visible as financial loss or criminal activity.

This has direct relevance to anti-money laundering and counter-terrorism financing settings.

Many contemporary offences begin well before a financial transaction occurs. They are shaped by environments that enable manipulation at scale, weaken traditional trust signals, and reduce the time available for individuals or institutions to respond. By the time a transaction is identified as suspicious, the underlying harm has often already taken place.

I am therefore writing to support the direction of reform, while highlighting the importance of recognising how illicit finance is now produced. Strengthening the ability to act on high-risk mechanisms is an important step. Ensuring that those mechanisms are understood within the broader context of modern harm pathways will be critical to achieving meaningful outcomes.

This submission draws on sustained engagement across policy, community, and international contexts. It reflects direct exposure to how digital harms evolve in practice, how existing safeguards and response systems struggle to keep pace, and how these gaps can undermine safety, trust, and resilience.

1. Support for the Direction of Reform

The proposed power enabling AUSTRAC to restrict or prohibit high-risk mechanisms reflects a necessary shift toward earlier intervention.

Beyond Transactions: Addressing the Pathways to Harm in Modern Illicit Finance -

Submission to the Parliamentary Joint Committee on Intelligence and Security review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026

In the current environment, certain products and channels can be quickly adopted by criminal networks once proven effective. Where misuse is repeated, and harm can scale rapidly, delay increases risk.

High-risk mechanisms are unlikely to be defined by a single feature. More often, they emerge through a combination of characteristics, including rapid value transfer with minimal friction, weak or inconsistent identity assurance, repeat linkage to known scam or laundering typologies, and limited traceability across jurisdictions.

Clarifying these characteristics would support consistent and transparent use of the proposed power.

At the same time, maintaining confidence in its application will be important. Clear evidentiary thresholds, proportionate use, and regular review will help ensure that intervention remains targeted and responsive to changing risk conditions.

2. Financial Crime Is No Longer Linear

Traditional models treated crime and laundering as separate stages. That distinction is becoming less useful.

Many contemporary offences operate as integrated systems. A person may be targeted through deception, persuaded to transfer funds, routed through intermediary accounts, and moved across borders within hours. Each step forms part of a continuous process.

What appears as a transaction is often the final stage of a broader chain of exploitation.

These pathways frequently operate across jurisdictions and can take advantage of differences in regulatory settings and enforcement capability. Without coordination, there is a risk that activity is displaced rather than disrupted.

This reinforces the need for earlier intervention and more integrated responses.

3. Emerging Technologies Are Changing the Economics of Crime

Emerging technologies are increasing the efficiency of existing criminal activity.

Tools capable of generating convincing text, synthetic audio, or fabricated documentation reduce the effort required to conduct fraud. Automated systems allow targeting at scale, while personalisation increases success rates.

The result is a shift in the economics of crime. Smaller actors can now operate with a reach and impact that previously required larger networks.

At the same time, many financial and digital services operate in environments that prioritise speed and ease of use. Where safeguards introduce friction, there can be pressure to minimise them. This can create conditions where risk reduction is uneven unless expectations are clearly set.

Certain digital asset conversion pathways, particularly those associated with scam cash-out activity, also warrant continued attention where patterns of misuse are evident.

As the scale of deception increases, so too does the volume of illicit proceeds entering the system.

4. Intervention Windows Are Shrinking

Speed has become a defining feature of modern financial crime.

Funds can be transferred quickly, often across multiple accounts or jurisdictions before a victim fully understands what has occurred. Real-time systems and automated processes intensify this effect.

By contrast, reporting pathways, investigation processes, and recovery mechanisms often remain slower and more complex.

This creates a consistent imbalance. The system responding to harm is slower than the system causing it.

Victims frequently encounter fragmented reporting pathways and limited clarity about next steps. Where recovery outcomes are uncertain, this can compound harm and reduce engagement with formal systems.

Improving response speed will require coordination across AUSTRAC, financial institutions, law enforcement, and regulators. Faster intervention and clearer escalation pathways will be critical.

5. Vulnerability Is Being Targeted with Precision

Many contemporary fraud models rely on identifying people who are more likely to trust or respond under pressure.

This may include those experiencing grief, isolation, cognitive decline, financial stress, or low digital confidence.

In many cases, vulnerability is deliberately targeted because it increases the likelihood of success.

This changes how risk is understood. It is not only about systems being compromised. It is also about people being placed in conditions where exploitation becomes more likely.

Recognising this pattern within national risk assessments, and strengthening links with community and support sectors, will improve early identification of emerging threats.

6. Financial Abuse That Remains Hidden

Some forms of harm are difficult to detect because they occur within relationships or under coercion.

This includes forced transfers, identity misuse, and financial control linked to abuse. It may also involve threats or manipulation that prevent victims from reporting.

These situations often sit between categories. They may be seen as social issues, legal matters, or financial concerns depending on the context.

When harm does not fit neatly into one category, it can become less visible.

Designing systems that reflect how harm is experienced, rather than how it is classified, will improve detection and response.

7. Frontline Recognition Is Critical

Early signs of emerging scams and laundering activity often appear outside formal intelligence systems.

Bank staff, fraud teams, community workers, and regional networks are often the first to notice patterns.

Their observations can provide valuable early warning. Without regular updates and clear escalation pathways, those signals may be missed.

Treasury, AUSTRAC, and industry bodies should consider coordinated capability uplift programs across banking, payments, telecommunications, and community sectors.

8. Data Sharing and System Friction

Effective disruption depends on information moving quickly between institutions.

In practice, this can be limited by legal, technical, and operational barriers. Where information cannot move at a speed consistent with the risk environment, intervention opportunities narrow.

Reducing these barriers will be important in improving system responsiveness.

9. National Security and Broader Risk Context

Large-scale scams and illicit financial extraction affect more than individual victims.

They can reduce trust in institutions, discourage participation in digital systems, transfer wealth offshore, and create lasting financial and emotional harm.

At scale, these impacts affect confidence and resilience.

While much of the current focus is on scams and fraud, it is also important to recognise that mechanisms which obscure identity or accelerate value transfer may present risks across both organised crime and terrorism financing contexts.

10. Measuring Effectiveness

Clear outcomes will be important in assessing whether reform is working.

These may include reductions in scam losses, faster intervention times, improved recovery rates, disruption of mule account networks, and lower levels of repeat victimisation.

A focus on outcomes, rather than activity alone, will support stronger accountability.

Recommendations

To support the effective implementation of the proposed reforms, the following considerations are offered.

1. Clarify indicators of high-risk mechanisms
Develop clear guidance to support consistent identification of mechanisms that present elevated risk, including patterns of repeated misuse, weak identity assurance, and limited traceability.

2. Support proportionate and transparent use of powers
Ensure that the application of restriction or prohibition powers is supported by defined thresholds, regular review, and proportionate safeguards to maintain confidence in legitimate financial activity.

3. Improve speed of intervention across systems
Continue strengthening rapid response pathways, including account freezing, escalation processes, and coordination between AUSTRAC, financial institutions, and law enforcement.

4. Strengthen frontline recognition capability
Support coordinated capability development across banking, payments, telecommunications, and community sectors to ensure emerging scam and exploitation patterns are identified earlier.

5. Reduce barriers to information sharing
Address legal, technical, and operational constraints that limit timely data exchange between institutions, recognising that delayed information flow reduces the effectiveness of intervention.

Conclusion

I support the intent of this legislation and the direction it sets.

Criminal networks will continue to adapt, particularly where systems allow them to operate quickly and at scale.

The question is whether institutions can respond with equal agility.

The proposed powers strengthen that capacity. Their effectiveness will depend on how well they are supported by faster operational pathways, stronger frontline capability, and a clearer understanding of how harm is now generated.

In many cases, what we are seeing as financial crime is not the starting point; it is the final stage of a much longer process of engineered exploitation.

The challenge is no longer whether criminal networks will exploit emerging systems; they already are. The real question is whether our institutions can recognise and respond to those patterns before harm becomes routine.

Warm regards,

[redacted]

Sarah Barnbrook
Founder and CEO
Away from Keyboard (AFK) Inc.
[redacted]
info@afk.org.au