No Bank Left Behind: Why Australia's Smaller Financial Institutions Are Critical to the Fight Against Child Sexual Exploitation

July 2026

As organised crime groups and individuals continue to exploit technology, child sexual exploitation and abuse (CSEA) is becoming an increasingly urgent and borderless crime. From tech-savvy criminal groups, like The Yahoo Boys running sextortion scams out of Nigeria, to people in our own backyard purchasing live-streamed child sexual abuse material (CSAM) from the Philippines, these abhorrent acts start with a child, and behind many of them is a financial transaction that has moved through an Australian bank.

Since 2022, sextortion investigations alone have led to the closure of thousands of Australian bank accounts, a staggering figure that represents only one form of CSEA-related crime. The sheer volume of these detections point to a wider landscape of CSEA offending that leaves financial footprints. When combined with other data, financial intelligence becomes a vital piece of the puzzle in identifying offenders and bringing them to justice.

1800+

accounts have been shut down under Operation Huntsman

(AUSTRAC, 2024)

Purchases of CSAM, importation of child-like sex dolls, travelling to offend, sextortion, and self-generated material (where children are coerced into producing content for payment) can all be identified by financial institutions through diligent transaction monitoring.

Australia's financial intelligence infrastructure is growing stronger – government agencies, financial crime professionals, law enforcement and non-governmental organisations (NGOs) are all working diligently to uncover these payments. Under the *Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act*, banks must actively monitor for suspicious transactions. However, offenders continually exploit gaps in the system to avoid detection. That is why it is imperative that financial institutions of all sizes have the awareness, intelligence, and networks they need to prevent, detect, and disrupt CSEA.

While Australia's major banks have dedicated financial crime teams and sophisticated technology, smaller institutions, including customer-owned and regional banks, often face this moral and regulatory obligation with far fewer resources.

The complexity of CSEA payments

The CSEA payment ecosystem is made up of three key groups: offenders, victims, and facilitators. Offenders are individuals driven by the desire to commit CSEA and consume CSAM - they enable the abuse to occur. Victims appear in various roles, especially in cases of sextortion. They may make payments to sextortionists or be coerced into acting as money mules. Vulnerable or financially disadvantaged children may receive payments directly from offenders for self-generated CSAM. In some typologies, such as live-streamed abuse, facilitators profit by arranging or enabling exploitation, acting as intermediaries who benefit financially from CSEA. Most important to mention is that all of these roles can appear in your customer base.

Detecting payments linked to child sexual exploitation is challenging, as offenders deliberately take steps to hide their activities, often paying small amounts and moving money through various financial systems to obscure their trail. This creates only breadcrumbs, making it nearly impossible for a single financial indicator to confirm if an account is being used for these purposes, or for any one entity to see the complete picture. However, when certain behaviours and patterns accumulate, they can signal that this activity may be occurring. Financial crime teams need to leverage data and intelligence to establish what constitutes normal behaviour, so they can better identify anomalies that may indicate criminal activity.

AUSTRAC gathers and analyses data submitted by financial service institutions through suspicious matter reports (SMRs), generating financial intelligence that supports law enforcement investigations. With AUSTRAC receiving over 450,000 SMRs in 2025, it's imperative that these reports are as robust and specific as possible to escalate an investigation. According to AUSTRAC CEO Brendan Thomas, "Every report is an opportunity to stop a potential offender, stop the flow of dirty money and protect vulnerable children from abuse."

AUSTRAC received
450,000
suspicious matter reports in 2025

(AUSTRAC, 2026)

> **Every report is an opportunity to stop a potential offender, stop the flow of dirty money and protect vulnerable children from abuse."**
>
> Brendan Thomas

AUSTRAC's own casework illustrates how these financial breadcrumbs translate into real outcomes. In one example, a man was identified as sending money to a known CSEA facilitator based in the Philippines. Analysis of his transaction history showed he had spent more than $50,000 over six years to purchase CSAM. He was intercepted by the Australian Border Force and the Australian Federal Police when returning from Bali in May 2023 and was arrested for possession and production of exploitation material found on his devices.

AUSTRAC supplied additional financial intelligence that supported his prosecution and helped identify other members of the network. The man pleaded guilty to seven child abuse charges in March 2024, and two of his victims were rescued from an alleged brothel in the Philippines.

There are several publicly available resources that banks can use to identify signs of CSEA in their transaction monitoring systems, including documents from AUSTRAC, the Financial Action Task Force (FATF), and privately available industry resources. However, detecting this activity can very much be a test-and-learn process. Transaction monitoring rules cannot be simply set and forget, they require ongoing optimisation. As a result, small and mid-sized banks often need access to intelligence and data beyond what they can usually gather independently. That is why information sharing within the sector, while already underway in some cases, can always be strengthened to further support these efforts.

Larger financial institutions have a unique opportunity to make a difference. As Doug Boudry, Non-Executive Director at ICMEC Australia, stated, organisations must **"find their way to yes"** by building trust-based partnerships with other institutions to drive real action.

NAB is an example of what large bank leadership in this space can look like. The bank developed a human impact guide that maps CSEA typologies and the financial indicators associated with them and has generously made this resource available to smaller institutions through ICMEC Australia's Financial Crime Collaboration Working Group (CWG). It is precisely the kind of knowledge transfer that moves the whole sector forward.

Understanding the resouce gap

Customer-owned banks and credit unions were created to serve specific communities and trades. While mergers have led to consolidation and fewer institutions, their assets have grown year on year. According to a 2025 study from KPMG, the sector held $178.4 billion in assets, up 5.8% from 2024.

To paint a picture of the resource asymmetry, Westpac, Australia's largest bank, had over 35,000 employees in 2025 and holds over $1.15 trillion in assets. In contrast, the COBA 2024 Impact Report found that customer-owned banks collectively employ over 11,500 full-time staff, while the smallest banks employ under 20.

Assets for customer-owned banks and credit unions equal
$178.4 billion
(KPMG, 2025)

Westpac has **35,000** employees
(IbisWorld, 2022)

Customer-owned banks have **11,500** employees collectively
(COBA, 2024)

Smaller institutions have to navigate a landscape of complex and competing priorities. CSEA is one of many issues demanding attention. From the growing number of scams and identity theft to drug trafficking, tax evasion, and more. Despite these challenges, regulatory requirements remain consistent, no matter the institution's size or how many staff they can dedicate to investigations.

Bronwyn Mead, Data & Intelligence Manager for Financial Crimes and Cyber Resilience at COBA, notes that the risk is there, regardless of size. She highlights that industry collaboration enables smaller institutions to uplift their knowledge and detection capabilities, helping them bridge the resource gap.

Mead also points out that the community focus of customer-owned banks presents a unique opportunity: "Customer-owned banks are often best placed to recognise CSEA behavioural factors which may not present in transaction monitoring alone because of their close connection to the communities they serve."

> **Customer-owned banks are often best placed to recognise CSEA behavioural factors which may not present in transaction monitoring alone because of their close connection to the communities they serve."**
>
> Bronwyn Mead

As community-focused entities, trust remains a key priority for the mutual sector. These institutions serve regional, rural and underserved communities - communities where trusted local banking relationships may make detection more possible, but where compliance infrastructure is thinner, operating with smaller teams and relying on sometimes fragmented or less advanced systems, opening exposure to threats.

Small institutions, significant impact

Despite the challenges, many smaller financial institutions are leaning heavily into CSEA detection strategies. At ICMEC Australia, the CWG brings together financial institutions of all sizes in a closed-door forum that elevates participants capability to combat CSEA by providing new information, data-driven projects and insights. The CWG offers a trusted space for attendees to collaborate, share expertise, and co-design solutions that strengthen collective defences and uplift detection of CSEA.

Hume Bank, a customer-owned regional bank headquartered in Albury-Wodonga, is an active participant in the CWG, and has generously provided guidance to other small institutions by presenting at the ICMEC Australia *Empowering Every Bank* webinar series and the ICMEC Australia 2025 annual Symposium. According to Ainslea Milthorpe, Financial Crime Compliance Lead at Hume Bank, collaboration is at the heart of their approach: "every financial institution, regardless of size, has a role to play, because each holds a piece of the puzzle." By sharing resources, intelligence, and insights, small banks like Hume Bank are able to connect the dots, take meaningful action, and protect children from harm. Milthorpe notes that "meaningful impact doesn't always come from having more resources; often, it's about getting creative, working together, and taking action."

> **Every financial institution, regardless of size, has a role to play, because each holds a piece of the puzzle. [...] meaningful impact doesn't always come from having more resources; often, it's about getting creative, working together, and taking action."**
>
> Ainslea Milthorpe

Hume Bank is not just a financial institution, but an integral part of the regional community in which they serve, with staff who live and work within the community and a great example of what a values-driven regional institution can achieve with the right culture, intent and tools.

This year, ICMEC Australia also welcomed Beyond Bank into the CWG. As a community-focused institution, Beyond Bank’s purpose extends beyond traditional banking - prioritising the protection of the communities it serves. Mark Wilson, Head of AML/CTF and Financial Crime at Beyond Bank, highlights that CSEA, including offences like sextortion, represents some of the most serious harms that can be enabled through financial systems. For Beyond Bank, identifying and disrupting the financial flows that support these crimes is a core commitment. Every action the bank takes to prevent abuse helps safeguard children and upholds the values of trust, integrity, and social responsibility that define the organisation. Wilson will share further insights on what transaction data can reveal from a small bank perspective at this year’s Symposium.

Why every bank must stay alert

The prevalence of CSEA offending is much higher than most realise, and pervasive across all communities, with 1 in 4 children in Australia having experienced CSEA (ACMS 2023). As a financial crime professional, there is every chance you have an offender cohort or victim-survivors as part of your customer base. Financial transaction data is crucial for law enforcement to build a comprehensive understanding of CSEA activity, making the role of financial crime professionals vital in both apprehending offenders and protecting vulnerable children.

1 in 4

Australians have experienced child sexual exploitation

(ACMS, 2023)

Offenders are proactive — they will look for the easiest way to exploit the financial system. When larger institutions identify and debank high-risk individuals, offenders may shift their activities to smaller institutions, which they perceive as having less friction for detection.

Additionally, offenders are highly networked, sharing tips and strategies on the dark web. No financial institution wants to become the "bank of choice" for these criminals, which is why it is critical for smaller institutions to remain vigilant and diligent in monitoring for this crime type.

A broader issue

For smaller financial institutions, it can be tempting to view CSEA detection as solely the domain of the financial crime team. But the reality is that CSEA touches many parts of a bank's operations.

Sextortion is also a scams issue. When a young person is blackmailed into paying a criminal, that transaction may present as a scam before it appears on a financial crime radar. Frontline customer service staff - the people answering phones, responding to branch enquiries, and managing online chats - may be the first to hear from a distressed young customer who doesn't yet know how to describe what is happening to them. Training staff on how to handle these moments can mean life or death and is as important as any transaction monitoring rule.

Product design matters, too. Robust customer onboarding and due diligence processes are among the most effective tools for preventing offenders from using a financial institution's products in the first place.

Finally, CSEA sits squarely within the social pillar of environmental, social and governance (ESG) frameworks. For customer-owned and mutual banks, the protection of vulnerable community members, particularly children, is not a compliance obligation sitting at odds with their values. It is an expression of them. Boards and leadership teams that have not yet considered CSEA within their ESG frameworks have an opportunity to do so.

Fighting CSEA is *everyone's* responsibility

Why larger banks must share knowledge to fight CSEA

CSEA is a challenge no single institution can tackle alone. Suspicious matter reports, transaction patterns, and shared intelligence all help law enforcement piece together activity that might otherwise go undetected.

For smaller financial institutions, the challenge is not a lack of commitment. Regional, customer-owned, and mutual banks face the same obligations as larger institutions, often with smaller teams, competing priorities, and limited access to intelligence. Recognising these realities is not about singling out smaller institutions, but about identifying where additional support, collaboration, and information sharing can have impact.

Smaller institutions also offer distinct advantages: their community relationships, local knowledge, and trust-based customer connections provide valuable context for detecting suspicious activity. When combined with practical tools, timely intelligence, and trusted partnerships, these strengths significantly enhance the sector's ability to respond.

ICMEC Australia is committed to partnering with the financial crime community to build shared capability. Larger institutions play a crucial role by sharing intelligence, typologies, lessons learned, and practical approaches that help smaller institutions strengthen their detection and reporting.

Ensuring that institutions of all sizes have access to the knowledge, support, and partnerships they need will boost our collective ability to identify financial indicators of CSEA and better protect children from harm. If you have ideas to help the industry, or if you would like assistance connecting with other institutions to strengthen your efforts, please contact us. Together, we can drive progress and make a meaningful difference in the fight against child sexual exploitation and abuse.

About ICMEC Australia

We deliver targeted child sexual exploitation and abuse detection, disruption and prevention projects in Australia. We work directly with organisations - including financial institutions, tech, travel and tourism, law enforcement, government agencies and broader corporate - to strengthen the systems that protect children.

corporate@icmec.org.au www.icmec.org.au ICMEC Australia

Resources

Australian Transaction Reports and Analysis Centre (AUSTRAC). (2024). *AUSTRAC urges financial services to look out for child exploitation transactions*. https://www.austrac.gov.au/new-and-media/news/austrac-urges-financial-services-look-out-child-exploitation-transactions

Australian Transaction Reports and Analysis Centre (AUSTRAC). (2025). *Protecting children from sexual exploitation*. https://www.austrac.gov.au/protecting-children-sexual-exploitation

Australian Transaction Reports and Analysis Centre (AUSTRAC). (2025). *Combating sexual exploitation of children for financial gain*. https://www.austrac.gov.au/industry-and-business/education-and-resources/publications-and-resources/combating-sexual-exploitation-children-financial-gain

Australian Transaction Reports and Analysis Centre (AUSTRAC). (2026). *Changes to transaction reporting from 1 July 2026*. https://www.austrac.gov.au/changes-transaction-reporting-1-july-2026

Customer Owned Banking Association. (2024). *Impact Report 2024*. https://member.customerownedbanking.asn.au/storage/reports/coba-impact-report-2024-web-final-1729033034EvSGR.pdf

Financial Action Task Force (FATF). (2023). *Online child sexual exploitation*. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html

IBISWorld. (2025). *Westpac Banking Corporation – Company profile*. https://www.ibisworld.com/australia/company/westpac-banking-corporation/3/

KPMG Australia. (2025). *Mutuals Industry Review*. https://kpmg.com/au/en/insights/industry/mutuals-industry-review.html