SUPER MEMBERS COUNCIL

ABN 64 671 146 688
SUPER MEMBERS COUNCIL OF AUSTRALIA LIMITED

Suite 2, Level 18
150 Lonsdale Street
Melbourne 3000
Victoria Australia

info@smcaustralia.com
smcaustralia.com

18 September 2026

Attorney-General's Department
via portal: consultations.ag.gov.au/rights-and-protections/privacy-reform/

Privacy reform – Consultation on Exposure Draft legislation

The Super Members Council welcomes the opportunity to respond to the Attorney-General's consultation on privacy reforms.

Harmful lead-generation models show how privacy failures can become devastating consumer harm. In the Shield and First Guardian scandal, more than 12,000 Australians lost around $1.2 billion of their retirement savings. This was not just a failure at the point financial advice was issued. The catastrophic harm began when the victims' personal information was harvested, shared and sold, and used to profile and draw people into engineered sales funnels that put their life savings at risk.

Lead generation (collecting information about prospective consumers and then converting it into commercial leads) and using or selling those leads to target people for financial products or services was central to the sales funnels that caused this harm. Stronger privacy protections are therefore an important preventive safeguard, particularly where personal information is collected, disclosed or used to target consumers with financial services marketing, and this is the basis for SMC's submission.

While this consultation necessarily addresses data collection, sharing and trading across the economy, SMC's submission focuses on how these practices operate in superannuation, financial advice and related financial services. It identifies where the proposed reforms could better prevent harmful data-driven sales funnels, while recognising that some of the risks created by lead generation models require major and substantive reform through the Treasury portfolio, not exclusively through Privacy Act reform.

This distinction matters. Privacy reform, while crucial, is not a complete answer to lead generation. Privacy reform is just one important part of a comprehensive response. The most serious harm in lead generation activities arises from commercial conduct that steers people towards high-risk financial decisions. The proposed privacy reforms reduce upstream risk without going far enough to truly protect Australians from dangerous clickbait advertising, predatory marketing and high-pressure sales funnels.

Australians save for a dignified retirement through a compulsory system over their working life, and where those savings are lost through harmful conduct, they may have no realistic opportunity to rebuild them. The law should therefore provide strong, preventative safeguards before irreversible harm occurs – which is why SMC considers privacy reform necessary but insufficient on its own and urges Government to progress comprehensive restrictions on lead generation alongside it.

SMC makes nine recommendations to the Privacy Act reform consultation, focused on combatting the harm caused by unscrupulous lead-generation activities and ensuring the reforms can be implemented coherently across superannuation and financial services. SMC recommends:

- stronger consent requirements;
- tighter limits on the secondary use and trading of personal information collected through comparison tools and promotions;
- heightened protections against harmful profiling and high-pressure marketing;
- accountability that follows personal information across the full lead-generation chain, backed by clear record-keeping;
- clearer and more robust records of personal information flows;
- close engagement with Treasury on how the reforms interact with lead generation;
- an implementation period that allows the OAIC to issue practical guidance before regulated entities must comply;
- resolution of conflicts and duplication between the privacy reforms and obligations applying to superannuation and financial services entities; and
- review of the proposed 72-hour data breach notification period to ensure it operates coherently with other regulatory reporting regimes.

SMC recognises that, as a cross-sector framework, the Privacy Act may not be the vehicle for sector-specific measures. However, the scale and irreversible nature of the catastrophic losses associated with Shield and First Guardian warrant targeted action. SMC urges Treasury to work closely with the Attorney-General's Department so that privacy protections and comprehensive financial services regulation reforms operate together to much better protect Australians' retirement savings.

About the Super Members Council

We are a strong voice advocating for the interests of more than 12.5 million Australians who have over $1.9 trillion in retirement savings managed by profit-to-member super funds. Our purpose is to protect and advance the interests of those millions of super fund members throughout their lives, advocating on their behalf to ensure super policy is stable, effective, and equitable. We produce rigorous research and analysis and work with Parliamentarians and policy makers across the full breadth of Parliament.

SMC recommends that the Attorney-General's Department:

1) Strengthen consent provisions so consent cannot be manufactured or used to legitimise harmful data-harvesting business models, including by requiring express, standalone and time-limited consent for the collection, use, disclosure or trading of personal information for lead generation, referral or financial services marketing.
2) Toughen restrictions on secondary use, disclosure and trading of personal information so information collected through comparison tools, promotions or online prompts cannot be reused, sold or disclosed for super switching, retirement savings marketing or financial advice lead generation where that use is outside the consumer's reasonable expectations or is likely to expose the person to financial harm.
3) Heighten profiling and vulnerability protections so entities must not use collected, purchased or inferred personal information to identify, segment, prioritise or target consumers for financial services lead generation or retirement savings marketing when doing so is reasonably foreseeable to expose the person to financial harm, unless the entity can demonstrate it has implemented effective safeguards to prevent that harm.
4) Ensure the privacy provisions apply across the full lead-generation and financial services marketing chain, with accountability following personal information whenever it is bought, sold, transferred, disclosed or used. Each entity should be independently responsible for ensuring its handling of the information is fair and reasonable, consistent with the consumer's original consent and expectations, and appropriately documented.
5) Strengthen the direct marketing provisions so opt-out rights are clear, simple and effective across the full marketing chain, and so collected, purchased or inferred personal information cannot be used to drive high-pressure financial services marketing that may put retirement savings at risk.
6) Require each entity involved in lead generation, referral arrangements or financial services marketing to maintain clear records of personal information flows, be accountable for whether its collection, use or disclosure is fair and reasonable in the circumstances, and disclose this information to the regulator as part of good governance.
7) Provide an implementation period that commences after the OAIC has published practical guidance, allowing entities sufficient time to assess and implement the final reforms.
8) Identify and resolve conflicts, duplication and uncertainty between the reforms and obligations applying to superannuation and financial services entities, including under the Retirement Income Covenant, the Spam Act 2003 and the Anti-Money Laundering and

Counter-Terrorism Financing Act 2006.

9) Review the proposed 72-hour eligible data breach notification period to ensure it is workable and aligned, as far as practicable, with other regulatory reporting regimes, avoids duplicative notifications and allows initial reports to be supplemented as material facts become available.

How privacy failures enabled retirement savings harm

The Shield and First Guardian disasters were not simply failures of financial advice given at the final stage of a consumer interaction. They exposed a broader chain of consumer harm that began much earlier, when people were drawn into lead-generation funnels through comparison tools, social media advertising, and online promotions that appeared helpful, neutral or low risk. By the time advice was provided, much of the damage had already been enabled. The consumer had been identified, targeted, and steered towards a pathway that put their retirement savings at risk. And consumer consent was manufactured in a bid to bypass both the spirit and letter of anti-hawking laws.

A high-risk consumer trajectory often starts with the harvesting of personal information, including contact details and indicators of financial interest or concern. That information can then be shared, profiled and reused across a commercial chain (including for super switching campaigns) long before the consumer understands who has their data, why they have it, or how it will be used – and the dangers that it poses to them for others to have that information about them. This means privacy regulation has an important preventive role in minimising consumer harm. Stronger privacy protections should not only respond to misuse after harm has occurred – they should also reduce the ability of harmful actors to assemble, trade and exploit data-driven sales pipelines in the first place.

In the Shield and First Guardian context, the privacy failure was that personal information could be converted into a commercial sales lead and used to propel consumers towards high-risk financial decisions about their compulsory retirement savings. Privacy law should therefore seek to prevent personal information from being converted into commercial leads, limit its reuse beyond consumers' reasonable expectations, and ensure that every entity involved in the data-sharing chain can be held liable and accountable for how that information is collected, disclosed and used.

Meaningful consent

SMC supports the proposed amendments to strengthen the definition of consent to collect personal information, including the requirement that consent be voluntary, informed, current, specific and unambiguous. These changes are an important improvement on the current framework.

However, stronger consent requirements are unlikely to address the privacy failures that are central to harmful lead-generation models. The Shield and First Guardian disasters show that consumer harm can begin at the point personal information is first collected. The relevant framework in the Corporations Act did require consumers to consent to being contacted, and many of the lead-generation models had various notional consent processes in place. In the Shield and First Guardian cases, consumers may have technically consented to data collection or follow-up contact, but that consent would likely never have been given if they had been required to be told that their information was about to be converted into a commercial lead, passed through multiple entities, profiled, reused and used to steer them towards high-risk decisions about their retirement savings.

ASIC's and the ACCC's own research show why strengthening the definition of consent will not, on its own, prevent harm of the kind seen in Shield and First Guardian. The ACCC's 2019 Digital Platforms Inquiry found that consent is routinely undermined by bargaining power imbalances and "clickwrap agreements with take-it-or-leave-it terms" that bundle multiple consents, and that representations about consumer control and choice often overstate consumers' ability to meaningfully control how their information is collected, used and disclosed. Research jointly published by ASIC and the Dutch Authority for the Financial Markets similarly found that disclosure and consent-based safeguards in retail financial services can be less effective than expected, or ineffective, in influencing consumer behaviour and may in some cases backfire and contribute to consumer harm. Although neither finding concerned lead generation specifically, both describe the dynamic evident in Shield and First

Guardian: consumers may have technically consented to contact or data collection in circumstances where consent could not be relied on to produce genuine understanding or control. Strengthening the definition of consent addresses the form of that failure; it does not address the substance.

Strengthening consent requirements is appropriate in an economy-wide privacy framework. Yet what is needed to avoid the predatory conduct witnessed in Shield and First Guardian is not more consent. To protect members while Treasury advances comprehensive approaches to lead generation, SMC considers that, for consent to be effective in this context, the law should require fully informed, express, standalone and time-limited consent covering the collection, use, disclosure or trading of personal information for lead generation, referral or financial services marketing. Consumers must understand how their information will be used. The hawking prohibition in the Corporations Act already prohibits unsolicited contact unless the consumer consents to the contact. The consent requirement is detailed and includes, among other things, that consent be voluntary, positive, specific and time limited. While finalising these privacy reforms, the Government should recognise that, although consent is a useful safeguard, it will not on its own protect consumers from harm in high-risk contexts such as super switching.

Consent should also not be treated as voluntary where access to a comparison tool, calculator, promotion or online service is effectively conditional on agreeing to broad downstream uses of personal information. Consent is also not informed when consumers are told only in general terms that their information may be shared with “partners”, “trusted providers” or “specialists”, without being told the practical effect of that sharing. These cases highlight the risk of “manufactured consent”, where consumers technically agree to the collection or sharing of their information but do so in circumstances where the practical effect, downstream use and number of entities involved cannot be genuinely understood. In lead-generation models, this means consent may satisfy formal requirements while failing to provide meaningful consumer protection.

SMC considers that consent and disclosure obligations need to be balanced and practical if they are to provide meaningful consumer protection in this framework. Disclosure and consent processes in financial services are already lengthy and complex, and adding further layers of warning language risks shifting responsibility onto consumers without improving their ability to understand what is happening to their information. This is particularly important where consumers are effectively required to waive control over their personal information to access a comparison tool, calculator or “super health check”, often through fast-moving online or telephone interactions. In those circumstances, a technically compliant consent process may still not be meaningful if the consumer cannot realistically understand who will be sent or sold their information, how many times it may be reused, or how it may be used to target decisions about their retirement savings.

This is why SMC does not consider that disclosure and consent settings, even if strengthened, can adequately address the risks of harmful lead generation. In lead-generation models, the risks are inherent in the structure of the activity. Personal information is collected, converted into a commercial lead, passed through multiple entities and used to steer consumers toward high-risk financial decisions. The risk of harm is too significant, and the data-handling chain too unclear, for consumer understanding to be achieved through longer disclosures or more detailed consent notices. Privacy reform should therefore support stronger consent and transparency requirements, while recognising that targeted restrictions on the collection, trading, reuse and onward disclosure of personal information for lead generation in relation to high-risk areas, such as superannuation, are needed to prevent harm before it occurs.

SMC therefore recommends that the consent provisions be strengthened so they cannot be used to legitimise harmful data-harvesting business models while Treasury prioritises substantive lead-generation prohibitions. At a minimum, the reforms should require fully informed, express, standalone and time-limited consent covering the collection, use, disclosure or trading of personal information for lead generation, referral or financial services marketing. Plain English warnings should be required to tell consumers clearly if their data will be sold to other parties.

Restrictions on data-sharing and secondary disclosure

SMC supports the proposed reforms to clarify and strengthen the rules governing the collection, use and disclosure of personal information. In particular, the proposed fair and reasonable test, the clarified meaning of “collects” and “disclosure”, and the proposal that organisations must not trade in personal information without consent unless an exception applies are reforms that go directly to the privacy risks that can arise as personal information is collected for one apparent purpose and then used or otherwise made available for a different commercial purpose.

These protections are particularly important in the context of lead generation. The Shield and First Guardian disasters demonstrate that consumer harm can be enabled by the movement of personal information through a chain of entities before financial advice is even provided. Consumers may initially provide information in response to a comparison tool, but that information can then be used to generate, qualify, sell or transfer a lead. In that context, the privacy risk arises from the onward use and disclosure of personal information across advertisers, lead generators, referral partners, callers, advisers and other intermediaries.

The proposed reforms are a useful step towards stronger regulation as they recognise that personal information may be obtained from third parties, publicly available sources, or generated or derived through data analysis and other technological processes. The proposed definition of disclosure is also important because it makes clear that personal information is disclosed when it is made accessible to another person or body, even where the original entity retains some control over it. This is critical to lead-generation models, where consumer data may be passed through multiple entities in ways that are not transparent to the consumer and may be difficult to trace after the initial interaction.

However, stronger safeguards are needed to address data-sharing and secondary disclosure in lead-generation chains, where the use of personal information creates a heightened risk of consumer harm. General statements that information may be shared with “partners”, “trusted providers” or “specialists” should not be sufficient to authorise onward sharing where the practical effect is to place a person into a commercial sales funnel.

SMC is concerned that a consent-based permission to trade in personal information may still allow harmful data-harvesting models to continue if the standard is satisfied through technical or “bundled” consent. In lead-generation contexts, consumers are unlikely to understand the full commercial chain, the number of entities that may receive their information, the purpose for which it may be reused, or the financial consequences that may flow from being targeted. Privacy reform should therefore ensure that consent to trade personal information does not operate as a safe harbour for business models that rely on opaque collection, repeated reuse, and onward disclosure of consumer data.

SMC recommends that the proposed restrictions on data-sharing and secondary disclosure be strengthened by requiring entities involved in lead generation, referral arrangements or financial services marketing to demonstrate the specific purpose for which personal information was collected, the entities to whom it was disclosed, and why each disclosure was fair and reasonable in the circumstances. The law should also make clear that personal information must not be reused or disclosed for super switching, retirement savings marketing, or financial advice referral pathways where the individual would not reasonably expect that use or where the use is likely to expose the person to financial harm.

This would preserve legitimate communications between super funds and their members while targeting the harmful commercial data practices that convert personal information into a sales lead. SMC’s position is that privacy reform should help stop harmful sales and data harvesting funnels from forming, not merely provide consumers with more information once their data has already entered the chain. Stronger restrictions on secondary use and disclosure are therefore essential to prevent consumer harm before retirement savings are put at risk.

The reforms should also preserve the ability of trustees and service providers to share personal information where reasonably necessary to prevent, detect or respond to fraud, scams, financial abuse or other serious wrongdoing. While stronger restrictions on harmful data-sharing for commercial purposes are essential, they should not inadvertently impede proportionate and appropriately safeguarded information-sharing that enables early intervention and protects consumers from harm, including where there are reasonable grounds to suspect financial abuse.

Profiling and vulnerability protections

SMC supports the proposed reforms insofar as they recognise that privacy risks can arise not only from the express collection of personal information, but also from the way information is analysed and used to target individuals. This is an important development. In modern data-driven business models, consumers may be profiled or targeted on the basis of information they did not knowingly provide for that purpose, including information that reveals or suggests financial stress, concern about retirement savings, uncertainty about superannuation, vulnerability to scams, or susceptibility to high-pressure marketing.

These risks were acute in the Shield and First Guardian lead-generation models and continue in lead generation today: apparently helpful prompts, social media advertising, and comparison tools can be

used to identify consumers before their information is converted into a commercial lead and used to steer them towards high-risk financial decisions. The information collected included dates of birth, contact details, superannuation balances and providers, employment and contribution status, investment knowledge and risk tolerance. Together, these data points were used to profile consumers and apply high-pressure sales tactics. Profiling is therefore not merely a privacy issue: it can be the first step in conduct that exposes compulsory retirement savings to significant harm.

SMC welcomes measures that clarify that sensitive information may be collected where it is inferred from other data. This is a useful safeguard, because harmful targeting practices do not necessarily rely on consumers expressly disclosing sensitive information. However, SMC considers that the proposed framework should go further to address profiling and targeting practices that expose consumers to financial harm, including where data used is not formally sensitive. A person may be vulnerable to harm because of the context in which they are targeted, the nature of the product or service being promoted, the complexity of the decision, the financial consequences of being moved through a sales funnel, or exposure to scams, coercion, financial abuse or misuse of substitute decision-making arrangements. In the superannuation context, targeting a person for switching, referral or financial advice lead generation can place their retirement savings at risk even where no sensitive attribute has been directly collected or inferred. Privacy settings should also enable entities to take proportionate action where there are indicators that a member may be experiencing financial abuse or other exploitation. Clear guidance on assessing harm, applying safety-by-design principles and determining appropriate intervention thresholds would support consistent application of these provisions.

The fair and reasonable test includes the risk of harm to the individual as one factor to be considered holistically. The legislation or explanatory materials should also make clear that collecting, using, disclosing, inferring or otherwise processing personal information will generally not be fair and reasonable where it is used to identify consumers for high-risk financial services lead generation, super switching campaigns, or retirement savings marketing that they would not reasonably expect, particularly where data flows are obscured or the practice is likely to exploit consumer uncertainty or vulnerability.

SMC also considers that profiling protections should not be limited to automated decision-making. Lead-generation models can involve a combination of digital targeting, algorithmic sorting, call-centre activity, referral arrangements and human sales conduct. A framework that only captures automated decisions may miss the practical way harm occurs. Privacy reform should therefore address both automated and non-automated profiling where personal information is used to identify, segment, prioritise or target consumers for commercial financial services pathways.

Stronger profiling and vulnerability protections would also help preserve the distinction between harmful lead-generation conduct and legitimate communications from a member's own super fund or employer. The objective should not be to restrict trusted communications that help members engage with their super. Rather, the framework should target unscrupulous commercial practices that use personal information to identify and move consumers into sales funnels that they do not understand and that may expose them to substantial financial harm.

SMC recommends that the reforms be strengthened so that profiling and targeting protections expressly address the use of personal information in financial services lead generation, referral and marketing models. Consistent with the fair and reasonable test, the legislation or explanatory materials should make clear that collecting, using, disclosing, inferring or otherwise processing personal information will generally not be fair and reasonable where it is used to identify consumers for high-risk financial services lead generation, super switching campaigns or retirement savings marketing that they would not reasonably expect, particularly where data flows are obscured or the practice is likely to exploit consumer uncertainty or vulnerability. This should include clearer guidance that entities must assess the likelihood of consumer harm, the vulnerability of the cohort being targeted, the complexity and significance of the financial decision, and whether the individual could reasonably understand and expect the way their information will be used. This would ensure privacy reform plays a stronger preventive role in stopping harmful data-driven funnels before consumers' retirement savings are put at risk. If this cannot be done as part of this review, it must be prioritised as part of further reforms to lead-generation activities.

Direct marketing reforms are necessary

SMC supports the proposed reforms to the direct marketing framework: in the context of super, the use of personal information for marketing can be the point at which a consumer is moved from passive online engagement into an active sales funnel that may ultimately place their retirement savings at risk.

In many lead-generation models, harm arises when collected information is used to target consumers with tailored marketing and sales approaches. A consumer may provide contact details or answer questions through a social media advertisement without understanding that the information may identify them as a prospective lead, prioritise them for follow-up and steer them towards high-risk financial products. The privacy framework should therefore treat direct marketing as a point of harm prevention, not merely a matter of notification and opt-out.

SMC supports reforms that strengthen consumer control over direct marketing and reduce the ability of entities to use personal information to drive high-pressure financial product marketing. This includes ensuring consumers have clear, simple and effective rights to opt out of direct marketing, and that those rights apply in practice across the full marketing chain. Opt-out rights will not be meaningful if they are difficult to exercise, apply only to one entity in a broader data-handling chain, or do not prevent the same information from being reused by another marketer, lead generator, referral partner or related entity.

SMC considers that additional safeguards are needed where direct marketing is based on collected, purchased or otherwise acquired data in the lead-generation ecosystem. Consumers are unlikely to understand the number of entities that may receive their information or the purposes for which it may be used. The direct marketing provisions should therefore make clear that personal information obtained from third parties, lead generators, data brokers or referral partners must not be used for super switching, retirement savings marketing or financial advice referral activity unless the use is fair and reasonable in the circumstances, within the consumer's reasonable expectations, and subject to clear and effective consumer control.

The reforms should also address marketing that relies on inferred information. Where inferred information is used to target consumers with financial services marketing, the risk is that consumers are selected precisely because they may be more responsive to clickbait advertisements, predatory marketing or high-pressure sales funnels. This is particularly concerning where the marketing relates to decisions about compulsory retirement savings.

SMC recommends that the direct marketing provisions be strengthened to ensure that entities cannot use collected, purchased or inferred personal information to target consumers with high-pressure financial services marketing in circumstances that are likely to expose them to harm. The framework should make clear that direct marketing practices are unlikely to be fair and reasonable where they involve unclear data flows, broad or technical consent, purchased leads, or repeated contact designed to move consumers into a financial advice or super switching pathway. This would align privacy reform with the consumer protection objective of stopping harmful funnels before Australians' retirement savings are put at risk.

At the same time, the reforms should preserve legitimate communications from a member's own super fund. SMC's concern is not with trusted communications that help members understand or engage with their superannuation. The concern is with commercial marketing models that harvest, buy, sell or infer personal information in order to identify consumers and steer them into unsuitable or high-risk products. The direct marketing framework should draw this distinction clearly, so that reforms target predatory marketing and high-pressure sales funnels while preserving legitimate trustee communications, member education and engagement activities that support informed decision-making and better retirement experiences.

Accountability across the chain

In lead-generation models, consumer harm can arise through the combined conduct of multiple entities, including advertisers, lead generators, referral partners, call centres, advisers and licensees. Accountability should therefore attach across the full data-handling chain, not only to the entity that first collects the information or the entity that ultimately provides financial advice.

The sale or transfer of personal information should not break the chain of accountability. An entity purchasing or receiving information should not be able to rely solely on assurances that consent was obtained earlier in the chain. It should be required to satisfy itself that the proposed use is consistent with the scope and purpose of the original consent, within the consumer's reasonable expectations, and fair and reasonable in the circumstances. Similarly, an entity selling or disclosing the information should remain responsible for taking reasonable steps to ensure that the recipient will use it consistently with those requirements. Clear responsibility at each transfer point is necessary to prevent accountability becoming fragmented as personal information moves through the lead-generation ecosystem.

Each entity should be independently responsible for ensuring that its handling of personal information is fair and reasonable in the circumstances. This includes being able to demonstrate why the information was collected, how it was obtained, to whom it was disclosed and whether its use was within the consumer's reasonable expectations. This information should be documented and retained for regulatory and good-governance purposes, with clear accountability where these obligations are not met.

Practical guidance from the OAIC will also be important to support consistent implementation of these obligations. The guidance should include examples illustrating how entities should balance fairness, individuals' reasonable expectations, transparency and the risk of harm across complex service-provider arrangements and member servicing environments.

SMC recommends that entities involved in lead generation, referral arrangements, or financial services marketing be required to maintain clear records of personal information flows and remain accountable to regulators for foreseeable consumer harm arising from their practices.

Implementation and interaction with other regulatory obligations

The reforms will require regulated entities to review their privacy frameworks, data inventories, consent and notification processes, contractual arrangements and incident-response procedures. SMC recommends an implementation period that begins only after the OAIC has had sufficient time to prepare and publish practical guidance. This would give trustees and other regulated entities a reasonable opportunity to interpret the final legislation, assess its operational implications and implement necessary systems and process changes consistently.

The Attorney-General's Department should also consider how the reforms interact with the duties and legislative requirements applying to superannuation and financial services entities. These include trustees' obligations under the Retirement Income Covenant, as well as requirements under the Spam Act 2003, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and associated regulatory frameworks. These regimes may require or support particular communications, information handling, member engagement and reporting practices. The final legislation and supporting guidance should identify and resolve any conflict, duplication or uncertainty so that privacy protections do not inadvertently impede trustees from meeting other statutory duties or communicating appropriately with members.

SMC further recommends that the proposed 72-hour period for notifying eligible data breaches be reviewed against the reporting thresholds and timeframes that already apply across financial services. A short statutory period may encourage early notification, but it should not require entities to provide incomplete or unreliable information before they have established the nature, scope and likely consequences of an incident. The final framework should align, as far as practicable, with other regulatory reporting regimes, avoid duplicative notifications and permit an initial notification to be supplemented as material facts become available.