Responding to identity theft: a systems analysis of actors, responsibilities, and vulnerabilities

Judy M. Watson[1,2], Gemma J. M. Read[1,3], Don Kerr[4] & Paul M. Salmon[1]

[1] Centre for Human Factors and Sociotechnical Systems, University of the Sunshine Coast, Qld, Australia, [2] School of Science, Technology and Engineering, University of the Sunshine Coast, Qld, Australia, [3] School of Health, University of the Sunshine Coast, Qld, Australia, [4] School of Business, University of Southern Queensland, Qld, Australia

SUMMARY

Responding to identity theft incidents is complex however our current understanding of the response system is limited. This study applied a systems analysis with the aim of identifying the actors that share the responsibility for victim outcomes following identity theft incidents in Australia. The findings identify a diverse set of 60 actor types involved in the response process and emphasise the lack of a single 'one-stop-shop' point of contact for victims. Recommendations for improvement are suggested.

KEYWORDS

Identity Theft, Systems Thinking, Risk Management Framework, ActorMap, Response System

Introduction

Identity theft is increasingly problematic resulting in economic and personal impacts that are detrimental to the health and well-being of victims (e.g. Watson, Lacey, Kerr, Salmon & Goode, 2019). Responding to an identity theft incident often involves multiple organisations and agencies, is complex, and takes time to resolve. In many jurisdictions the identity theft response system has been found to be sub-optimal. Research has acknowledged victim confusion in knowing how to remediate the crime (Green et al., 2020), and where the remediation process requires victims to contact more organisations/agencies, more non-financial impacts are experienced (Watson et al. 2019).

Previous research has called for a more holistic understanding of the identity theft response system to help mitigate the negative outcomes for victims (Watson et al., 2019). Such a holistic understanding could be gained through taking a systems thinking approach. A commonly applied systems thinking framework is Rasmussen's Risk Management Framework (RMF) (Rasmussen, 1997). The framework describes how actors (both human and non-human) reside at the varying levels of a system hierarchy and how overall system behaviour emerges through interactions between actors across the levels (see Figure 1). The framework is versatile, domain-generic, and easily modified for different complex problems that require investigation.

The RMF can be operationalised further for a domain by using the related ActorMap technique (Svedung & Rasmussen, 2002), which identifies the actors that reside within a particular system. It provides a graphical representation of the individuals, agencies and organisations who share

responsibility for the performance of the system. In addition to identifying human actors, previous applications have also included physical elements of the system such as equipment used and the broader surroundings in which interactions occur (e.g. McIlroy et al., 2019).

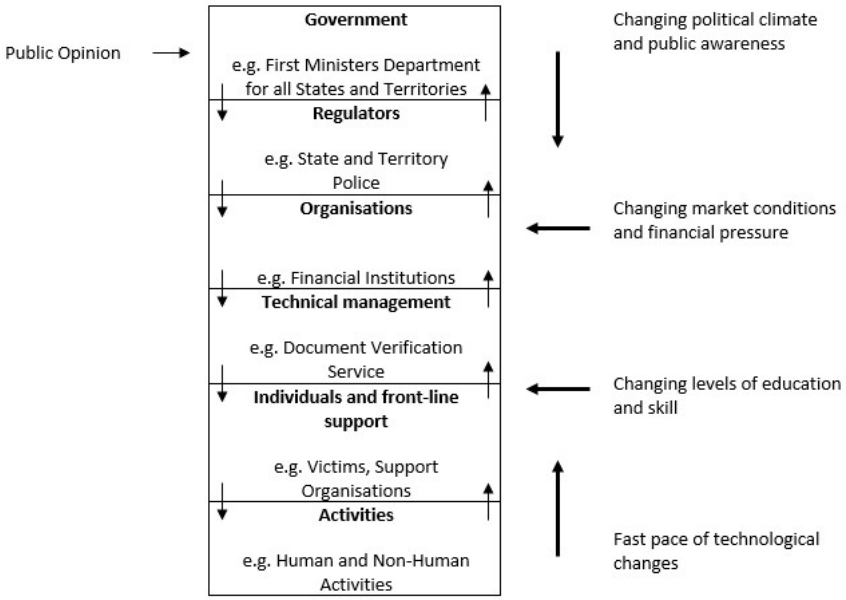

Figure 1: Hierarchical framework of the Australian identity theft response system. Adapted from Rasmussen (1997)

The aim of this study was to identify the actors within the identity theft response system, their responsibilities, and the physical elements that comprise the system, to inform opportunities to optimise the response system. It is important to note that the boundary of this study was limited to the identity theft response system within Australia. Whilst it is recognised that in certain circumstances the system may interact across international borders (e.g. where credit cards are used illegally in another country), interactions with international institutions were not the focus of this analysis.

Method

The ActorMap technique (Svedung & Rasmussen, 2002), was used to map and visualise the actors that reside within and share responsibility across the hierarchical levels of the identity theft response system. The initial ActorMap was informed by existing literature, websites and key agency policy and procedures. The actors and physical elements were mapped to the six different levels of the ActorMap (see Table 1 for descriptions).

Participants

The initial ActorMap was reviewed and verified by 12 subject matter expert participants of various actor types represented within the ActorMap. The participants either had subject matter expertise in the area of identity security and held a current role within the response system, had directly supported a victim following an identity theft incident, or were themselves a victim of an identity theft incident. Participants had expertise in privacy regulation, identity security/biometric policy, criminology and law, law enforcement, financial crime/fraud investigations/operational risk, cybersecurity, cybersecurity/consumer privacy/data security, and victim support. One participant had lived experience as a victim of identity theft.

Materials and Procedure

Participants were provided with a copy of the initial ActorMap and of the interview protocol prior to attending a semi-structured interview. During the interviews, participants were stepped through each level of the ActorMap and asked if each of the actors represented at the level in question should be moved, renamed, or removed. Participants were also asked to nominate all other actors with whom they interacted at each level of the ActorMap and whether, after modification, the reviewed level would represent a comprehensive description of the actors at that level. The feedback from participants was collated and used to amend the initial ActorMap. The following rules were applied:

- Addition of an actor to the ActorMap required that the proposed actor was an individual, agency or organisation that had a role within the response system.
- Movement of an actor to a different level was governed by the role of the actor. For example, for an actor to be moved from Government Actors (level 1) to Regulatory Bodies and Associations (level 2) the participant had to explain that the actor had regulatory powers.
- Removal of an actor required that the actor had no interaction with any other actor within the response system or that the actor was already included within/covered by another actor type within the ActorMap.
- Actors were renamed where it was advised that the agency/organisation had changed/updated its name.

When no further amendment advice was received, the model was finalised. Table 1: ActorMap levels and descriptions

Level	Description
Government actors	These actors are involved in informing and developing policy and regulations, delivering policy and providing strategic advice.
Regulatory bodies and associations	These actors perform compliance monitoring and enforcement roles to ensure that individuals, agencies and organisations comply with legislative requirements.
Organisational management actors	These actors provide a variety of services, such as supporting the Australian payment system[1]. A key role for many of the actors at this level is to issue and manage documents and/or accounts which hold identity information.
Technical and operational actors	These actors provide technical and operational support to other system actors. For example, Biometrics Service Providers provide software that enables the capture, storage and management of biometric identity information in a digital environment.
Individual and front-line support actors	These actors aid in achieving a specific requirement of the response process, such as a sworn testament. They offer various types of support, such as social support, health related support, or advice on response procedures. Victims are included at this level, as they take an active role in responding to identity theft incidents.
Equipment and surroundings	The objects at this level are the physical elements within the response system comprising equipment, products and the environments in which they are used.

[1] For example, the Australian Payments Network supports the payment system within Australia by collaborating with organisations with an interest in payments, to deliver improvements for system users (Australian Payments Network, 2022).

Results

A total of 60 actor types, whose roles and responsibilities vary, were identified (see Figure 2). These comprise 10 government actors, 12 regulatory bodies and associations, 18 organisational management actors, 10 technical and operational actors, and 13 individual and front-line support actors. Notably three actor types held more than one type of role/responsibility. A total of 22 objects were identified (see Figure 2).

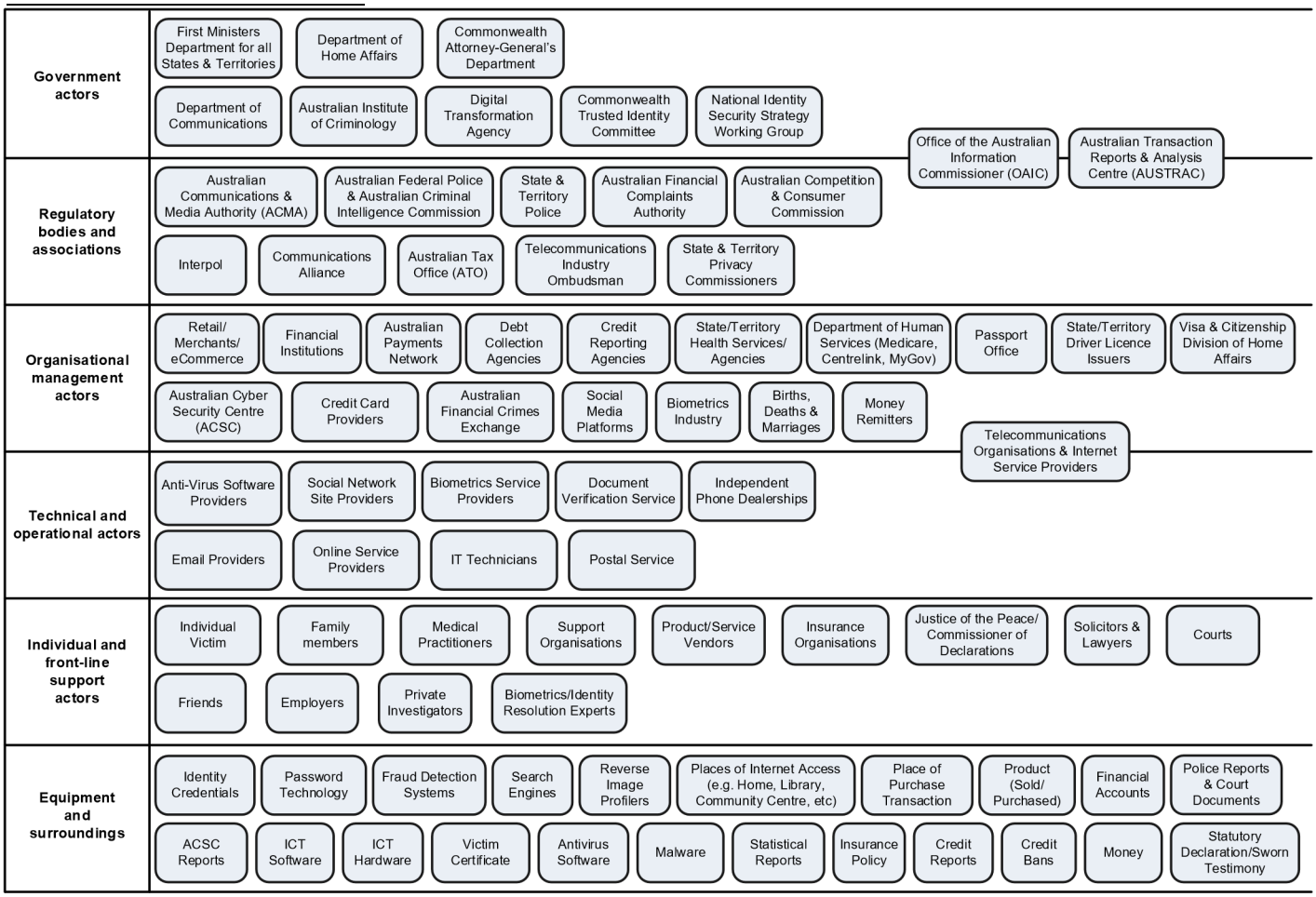

Figure 2: ActorMap – Actors responsible for responding to identity theft (Australia) **Discussion**

The aim of this study was to use the ActorMap technique to identify the actors that share responsibility for identity theft victim outcomes, as well as the physical elements that comprise the system, and to look for opportunities to optimise the response system.

A first key finding was that the large and diverse range of actors may be challenging for victims to navigate as they decide how to respond to an identity theft incident. The system comprises a complex set of actors with whom victims may choose to, or be required to, interact. For example, if an individual lost a wallet containing their credit card and their driver license, they would be required to report the loss to both of the issuing organisations. It would also be advisable for the individual to contact the credit reporting agencies to check their credit report to ensure that no loans

had been opened in their name. However, they may elect not to take this optional action (indeed, they may be unaware of it). This leaves them vulnerable to further misuse of their identity.

Given the diversity of actors identified within the ActorMap, it is worthwhile to consider where reporting is mandatory as opposed to optional. Based on previous literature (e.g. McAlister & Franks, 2021; Watson et al., 2019) and guidance available to victims of identity theft (e.g. IDCARE, 2022), Table 2 shows the actors identified in the ActorMap, to whom victims are required to report an incident to (n = 9) and those that they choose to inform for various other reasons (n = 27, including informal actors such as family members and friends). Prior research has acknowledged that a network of agencies and organisations are involved in the response journeys of fraud victims (e.g. Cross, Richards & Smith, 2016), that there is a confusing array of response opportunities (e.g. Button, Tapley & Lewis, 2012), and that victims are challenged when trying to report an incident (Cross, 2018).

Table 2: Actors to whom victims are required or may choose to report an incident

Required to report to:	**May choose to report to:**
1. Australian Tax Office	1. State & Territory Police
2. Australian Cyber Security Centre	2. Australian Federal Police & Australian Criminal Intelligence Commission
3. Financial Institutions	3. Australian Competition and Consumer Commission
4. Credit Card Providers	4. Australian Communications and Media Authority
5. Services Australia (formerly the Dept. of Human Services)	5. Births, Deaths, and Marriages
6. Passport Office	6. Credit Reporting Agencies
7. State/Territory Driver Licence Issuers	7. Debt Collection Agencies
8. Visa and Citizenship Division of Home Affairs	8. Email Providers
9. Telecommunication Organisations & Internet Service Providers	9. Employers
	10. Family Members
	11. Friends
	12. Insurance organisations
	13. IT technician
	14. Medical Practitioners
	15. Money Remitters
	16. Office of the Australian Information Commissioner
	17. Online Service Provider
	18. Postal Service
	19. Private Investigators
	20. Product/Service Vendors
	21. Retail/ Merchants/ eCommerce
	22. Social Media Platforms
	23. Social Network Site Providers
	24. Solicitors & Lawyers
	25. State/Territory Health Services/Agencies
	26. Support Organisations
	27. Telecommunication Industry Ombudsman

Overall, within the ActorMap a larger number of actors were identified at the organisational management level of the system. Many were agencies or organisations that issue identity documentation and credentials which enable and facilitate government and business operation

transactions where maintaining authentic, valid identity is essential. For example, if a credit card is compromised the victim would be required to interact with the financial institution who issued the card. In some cases, however, it may be difficult for a victim to know which agency to contact in relation to a comprise event. For example, if notified of the compromise by a debt collector in regarding a debt that they did not authorise, a victim may have difficulty identifying how their identity was compromised, and thus who to contact to resolve the issue. Further, victims may not report compromises of non-financial credentials to other issuing institutions, potentially not understanding the value and potential for misuse of other identity credentials. The greater number of actors at this level may account for the challenges faced by victims in complex identity theft situations where multiple credentials have been compromised. What is evident from the ActorMap is that there is no single 'one-stop-shop' point of contact for victims to report these types of incidents. Arguably it is not unreasonable for victims to think that by contacting a government agency or regulatory body, the agency/body will manage the reporting process on their behalf. For example, some victims may think that by contacting agencies such as the Australian Competition and Consumer Commission, through the 'Scamwatch' website, the resolution of their issue will be facilitated. Prior research conducted in Australia has reported victim confusion and disappointment with that reporting process as the victim reports were not individually investigated but used for data collection to inform prevention strategies (Cross et al., 2016). An actor with a victim-focused coordinating role which facilitates reporting identity theft incidents to credential issuers and related relevant actors could simplify the process and support victims.

A second key finding was that actors have a range of roles and responsibilities when responding to identity theft. Importantly, the focus of their responsibility may not always relate specifically to supporting victims to regain control of their identity. Given the response system operates alongside the transaction system where maintaining authentic, valid identity is essential for trust in commerce. These institutions are concerned with their own objectives around ensuring smooth business processes (Wyre, Lacey & Allan, 2020). These objectives include the assessment of creditworthiness and managing the risk of on-going fraud from the misuse of stolen credentials. Therefore, the response system holds various objectives outside of victim support. Not attending to the full range of responsibilities leaves the transaction system vulnerable and open to misuse and loss of trust. Further, credentials themselves are also used for various purposes. Facilitating certain transactions may be the primary purpose of specific identity credentials, such as driver licenses which are issued for the primary purpose of demonstrating legal authorisation to operate a vehicle. However, these may also be used for authenticating and validating identity in further situations, such as using driver license details to provide identity when establish a loan. Using identity credentials for this secondary purpose adds complexity to the situation and may confuse actor responsibilities. For example, when a driver license is compromised and used for illegally authenticating identity, where does responsibility towards the victim of the theft lie?

While the ActorMap identifies the actors that share the responsibility for the response to identity theft, it does not analyse the appropriateness of their roles or responsibilities. Research has noted that the prevention of identity theft is the responsibility of more than one type of actor (Piquero et al., 2021). However, to understand the appropriateness of the roles it is important to understand how the response system functions. It is also important to understand what response system actors consider they are responsible for. Further, it is vital to consider the role of the victim within the response system. Victims were included in the ActorMap as they play a key role in responding to identity theft through identifying and reporting identity theft incidents and managing the recovery of their credentials. They also play a role preventing on-going identity theft through the management of their credentials. As noted above, having one point of contact for victims to report

incidents to and to assist them to manage the recovery process would reduce the burden placed on this group (e.g. Watson et al., 2019), who may experience disadvantages in advocating for their needs due to language or cultural barriers, age or other factors (e.g. Burnes, DeLiema & Langton, 2021).

Limitations and Future Directions

While this study has documented the actors and physical elements within the identity theft response system, it has not gone further to consider in detail the functions undertaken by actors, nor has it defined the related constraints on behaviour. Further, the ActorMap technique does not capture communication or feedback loops between the actors. Future research might use methods such as the Systems Theoretic Accident Model and Processes (STAMP; Leveson, 2004) to understand the mechanisms used by actors to control and constrain the activities of others, and to provide feedback regarding the state of the system and the effectiveness of controls. The actors identified here could provide the basis for the development of a STAMP control structure model. Further, to achieve better understanding of the objectives of the actors and physical elements in the system, and actor roles and responsibilities, other additional systems thinking methods could be applied such as Cognitive Work Analysis (CWA; Vicente, 1999). CWA could assist to better understand the objectives, constraints, functions, roles and responsibilities of system actors and how these may be complementary or possibly contradictory. CWA could be used to identify opportunities to optimise the process of responding to an incident.

As the scope of this analysis was limited to the identity response system in Australia, future research should apply the ActorMap technique in other jurisdictions to assist in identifying issues and recommendations relevant to local contexts and enable cross-jurisdictional learning. Further, the ActorMap technique could be used to build global understanding of the actors that are involved in responding to identity theft incidents. This type of cross-country analysis has previously been undertaken in road safety system research, generating useful new insights in that field (McIlroy et al., 2019).

Conclusion

This research extends existing knowledge by using the ActorMap technique to identify the actors who share the responsibility for responding to identity theft within Australia. A diverse set of stakeholders were identified. The findings provide insight into the difficulties that victims experience, due to the large volume of agencies and organisations that they are faced with when reporting and resolving an identity theft incident. Recommendations include establishing a single ‘one-stop-shop’ point of contact for the victim. Overall, the study illustrates the benefits of considering the wider system when searching for holistic understanding of the complex problem of identity theft.

References

Australian Payments Network. (2022). *Convenient and secure payments for all.* Retrieved from https://www.auspaynet.com.au/

Burnes, D., DeLiema, M., & Langton, L. (2021). Identity theft and older adults: How minorities and the poor suffer the worst consequences. *Innovation in Aging, 5*(Supplement 1), 322-323. doi: 10.1093/geroni/igab046.1256

Button, M., Tapley, J., & Lewis, C. (2012). The ‘fraud justice network’ and the infra-structure of support for individual fraud victims in England and Wales. *Criminology and Criminal Justice, 13*, 37-61. doi: 10.1177/1748895812448085

Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, 55, 1–12. doi: 10.1016/j.ijlcj.2018.08.001

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and issues in crime and criminal justice, No. 518.* Retrieved from https://www.aic.gov.au/crg/reports/crg-2913-14

Green, B., Gies, S., Bobnis, A., Piquero, N. L., Piquero, A. R., & Velasquez, E. (2020). The role of victim services for individuals who have experienced serious identity-based crime. *Victims & Offenders, 15*, 720-743. doi: 10.1080/15564886.2020.1743804

IDCARE. (2022). *National Identity and Cyber Support*. Retrieved from https://www.idcare.org/

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science, 42*, 237270. doi.org/10.1016/S0925-7535(03)00047-X

McAlister, M., & Franks, C. (2021). *Identity crime and misuse in Australia: Results of the 2021 online survey. Statistical bulletin 37*. Retrieved from https://www.aic.gov.au/sites/default/files/2021-12/sb37_identity_crime_and_misuse_in_australia_results_2021_survey.pdf

McIlroy, R. C., Plant, K., Hoque, M. S., Wu, J., Kokwaro, G. O., Vu, N. H., & Stanton, N. 2019. Who is responsible for global road safety? A cross-cultural comparison of Actor Maps. *Accident Analysis and Prevention, 122*, 8-18. doi: 10.1016/j.aap.2018.09.011

Piquero, N. L., Piquero, A. R., Gies, s., Green, B., Bobnis, A., & Velasquez, E. (2021). Preventing identity theft: Perspectives on technological solutions from industry insiders. *Victims & Offenders, 16*, 444-463, doi: 10.1080/15564886.2020.1826023

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science 27*, 183–213. doi: 10.1016/S0925-7535(97)00052-0

Svedung, I., & Rasmussen, J. (2002). Graphic representation of accident scenarios: Mapping system structure and the causation of accidents. *Safety Science, 40*, 397–417.

Vicente, K. J. (1999). *Cognitive work analysis: Towards safe, productive, and healthy computerbased work.* Mahwah, NJ: Lawrence Erlbaum Associates

Watson, J., Lacey, D., Kerr, D., Salmon, P., & Goode, N. (2019). Understanding the effects of compromise and misuse of personal details on older people. *Australasian Journal of Information Systems, 23.* doi: 10.3127/ajis.v23i0.1721

Wyre, M., Lacey, D., & Allan, K. (2020). *The identity theft response system.* Retrieved from https://www.aic.gov.au/publications/tandi/tandi592