# Contextualized Cyber Security Awareness Approach for Online Romance Fraud

**Final Year Project by Sara Dickerson**

Bournemouth University

**Issue:** There is a need for an effective approach to drive increased awareness to address the growing issue of online dating scams and romance fraud.

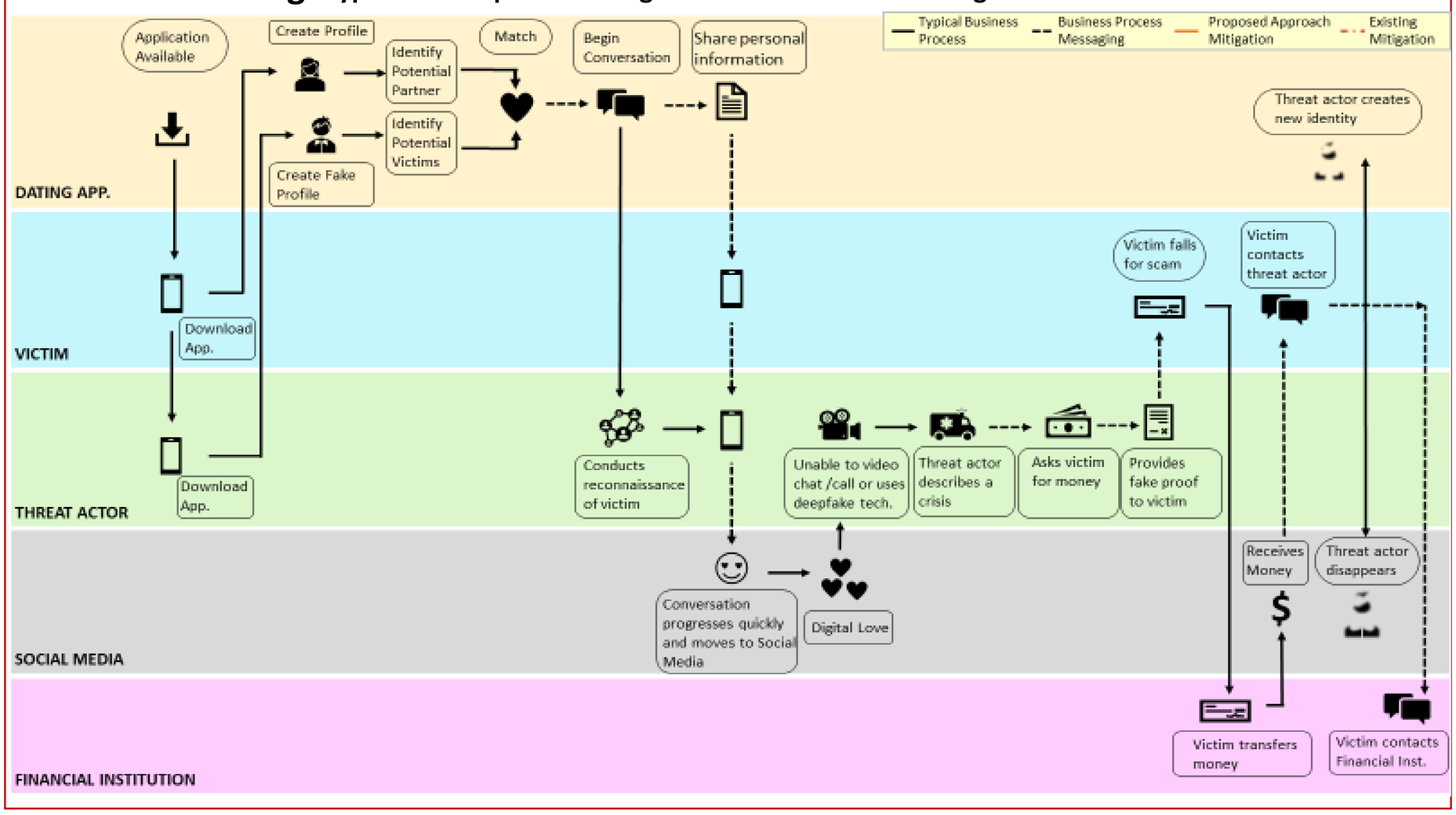
- **£50 million** was lost due to romance fraud in 2018. A **27%** increase in monetary loss from 2017.
- There were **4,555** complaints of Romance Fraud reported to Action Fraud in 2018.

(Action Fraud, 2019) (Action Fraud, 2018)

## Objectives:

- Use literature to investigate the current state of online romance fraud and existing detection and mitigation measures.
- Develop and implement a cyber security awareness approach
- Disseminate key findings of the study to relevant academics and industry stakeholders

## Process Modelling: Typical attack process using Business Process Modelling and Notation



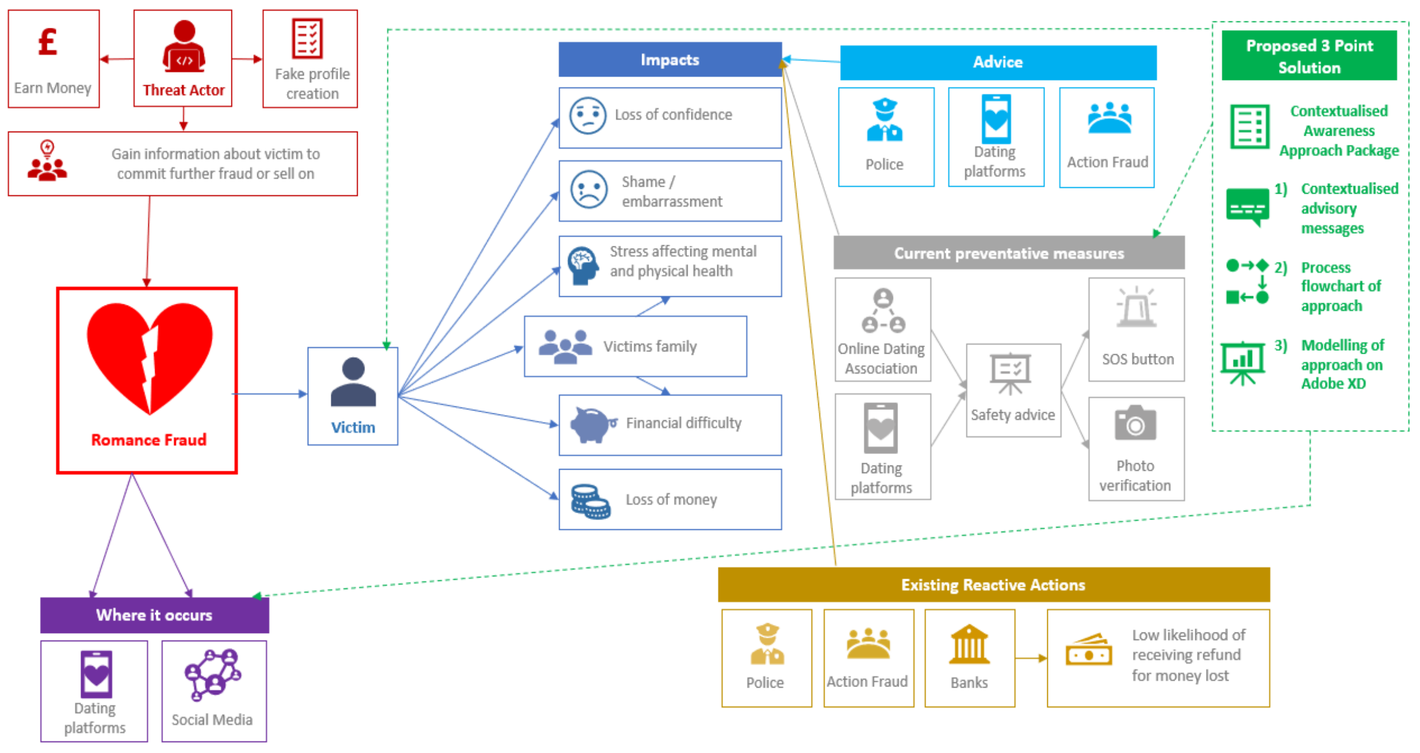

## Methodology:

- Use an agile approach for project management.
- Utilise a mixed method research approach, using both qualitative and quantitative data.
- Adopt and implement design tools, business process models and use cases to build persona models in order to analyse the current processes and establish the requirements and design for the approach.
- Demonstrate how the approach can be implemented by organisations, using Adobe XD to provide examples.
- Test and evaluate the approach by using focus groups comprised of users of dating platforms and academics.

## Findings

- There is currently no common tactical approach to increase the awareness of romance fraud to users of online dating platforms.
- Current awareness approaches occur primarily outside the platform through organisations such as Action Fraud.
- Existing mitigations in place focus on technological measures to prevent threat actors rather than educating potential victims.
- Technological countermeasures currently implemented by dating platforms include; an SOS button to improve physical security, photo verification tools to verify user profiles and updated security guidance.
- Third party organisations such as Scamalytics use machine learning, real time detection and shared blacklists to help monitor for fraudsters on online dating platforms (Scamalytics, 2019).
- Some users are taking matters into their own hands to detect fake profiles but may be putting themselves at further risk by sharing personal information.
- There is a need for increased awareness and early intervention to help potential victims.

## Rich Picture of Romance Fraud and Interventions




### Example of how the approach can be implemented


## Proposed 3 Point Solution

- A cyber security awareness approach looking at the current threat landscape and creating preventative mitigations tailored to psychological methods of personas which can be adapted and implemented by dating platforms to educate users of the indicators of romance fraud and social engineering techniques.
- Including an awareness package with example content and educational messages as well as detailing recommendations on identified at risk users and the context in which to display educational messages.
- Demonstrations, using Adobe XD, displaying how the approach can be implemented both within an app to help users and as a dashboard to help platforms track progress.

**References:**

- Action Fraud, 2018. *Victims lost £41 million to romance fraud in 2017.* [Online], Available at: https://www.actionfraud.police.uk/news/victims-lost-41-million-to-romance-fraud-in-2017, [Accessed 2019 10 24].
- Action Fraud, 2019. *Don't invest your heart in a fauxmance: victims lose over £50 million to romance fraud.* [Online] , Available at: https://www.actionfraud.police.uk/news/dont-invest-your-heart-in-a-fauxmance-victims-lose-over-50-million-to-romance-fraud, [Accessed 24 10 2019].
- Scamalytics, 2019. *Scamalytics.* [Online], Available at: https://scamalytics.com/, [Accessed 23 10 2019].