Financial abuse case study B:

MW is a lady in her 60s who has a learning disability. She lives in her own flat within a supported living structure of 9 other flats. She has lived within the same organisation for the past 20 years.

She had lived in a residential setting for all of her adult life and in 2013 moved from a residential setting into a supported living placement. She has her own front door and flat.

There is a 24/7 presence in her home and she receives support for most activities in both her home and accessing the community.

MW recently bought herself an Ipad to help her with ordering essentials due to her decreasing mobility. She has capacity to understand what the Ipad is used for and what she wanted it for. She is able to read a little and understands when something has been explained to her.

She learnt to use with support and was able to access the device to play games and browse independently. She has used her Ipad to purchase items that she has wanted and needed, this is generally with staff support.

Recently a purchase arrived for MW that was a handbag costing £160. When asked about it she knew nothing about it. An investigation took place.

Within the investigation it came about that although passwords and securities where locked away, all staff had access to those securities after accessing the locked room they were kept in. It also came to light that when accessing her Ipad her Amazon account was accessible as an app applied to her Ipad. The app on her Ipad wasn't password protected and she and anyone else using her Ipad had full access to her account. This included her card details as they were logged into the account.

From the investigation it appears that MW had been browsing through Amazon and something had come up that we would understand as 'something you may be interested in', however, MW was unable to correctly read and understand this statement, clicked on it and with the one click option bought the item.

Amazon were incredibly understanding and the item was returned and also the monies paid for that item.

Following this event, systems were increased to provide more security for both MW and other service users within the provider organisation's properties.

It was believed that security was sufficient in that staff were the only ones that had access to passwords, having them locked away from the eyes of others. Financial risk assessments were in place. Specific purchases were made with staff support via a support plan, budget planning and support session plans.

The learnings are significantly different to those that are usually expected with regard to financial abuse. They are based around safety and security when using electronic devices such as smartphones and tablets:

- Passwords were accessible to all staff
- Passwords are useless if they are not used each time – the Amazon account was open on the app
- Other people had access to MW's Amazon account if using her Ipad
- Financial risk assessment had no reference to electronic devices associated with making purchases
- Payment systems were saved within the account information
- MW would use her Ipad to browse without staff support.

What has happened since?

- All service users with electronic purchasing devices are supported to keep their password somewhere confidential and safe
- Passwords are to be entered to open apps etc
- Payment systems are NOT saved and are entered for each purchase made, this would be done with staff support for most of the service users living in our properties
- Financial risk assessments are updated to include electronic purchasing devices and the risk they may pose and what can be put in place to safeguard that risk
- All services have been informed of the risk and to implement safeguards mentioned above.