5 Software and Security Engineering (rja14)

You have been hired to design a mobile phone app for a brokerage firm, whose business is to help people to manage their investments. Their customers will use the app to check the prices of the shares and bonds that they own, sell them when they wish, and buy others. The customers' investment portfolios are typically worth six figures or more. You have already implemented industry standard mechanisms for the customer to authenticate to the app using the phone's biometric mechanisms, and for the app to authenticate itself to the broker's servers using TLS. Orders to sell investments, or to transfer sale proceeds from the customer's account at the brokerage to a bank account, also need a second authentication factor, as a requirement from the regulator. At present the brokerage sends an SMS message to the customer's phone.

The firm wants a recovery mechanism to support users who have lost their phone, bought a new one, and downloaded a new copy of the app. On initialisation, the app will generate a set of cryptographic keys, and send the public keys along with the phone's details to the broker, encrypted under the broker's TLS key. The recovery mechanism will authorise a new set of keys to be used to access an existing account and, together with the SMS second factor, to sell investments or withdraw the proceeds of sales.

(*a*) The brokerage firm first suggests sending an email to any customer who needs to recover an account, with an activation code to type into the app. Discuss the security, usability and cost of this option. [5 marks]

(*b*) Another suggestion is to rerun the initial 'know-your-customer' registration procedure which involves the customer sending the brokerage a photo of their passport or driving license plus two utility bills. Discuss the security, usability and cost of this option. [5 marks]

(*c*) Does the SMS second factor do any useful work? Justify your answer. [5 marks]

(*d*) What might you suggest that is better? Discuss its security, usability and cost. [5 marks]