

Risk analysis of banking agents

Ignacio Mas, CGAP Technology Program 2008

The following table lists a variety of risks that may in principle exist when a client-bank interaction is happening through a third party. For each risk, it lists some possible risk mitigation options and identifies which party assumes the residual risk if the risk in fact comes to pass. This table is merely illustrative; it is not meant to be a comprehensive list of all risks, nor of all the measures that need to be taken. It is only intended to show how for most risks that one can think of there is generally a potential technical solution; regulators and banks will need to decide what is the appropriate balance between risk minimization and cost and complexity of the technical solution.

Type of risk	Possible risk mitigation options	Who assumes residual risk
Theft of cash		
The client is robbed in or around the premises of the agent	<ul style="list-style-type: none"> Bank chooses agent based on security of location. Bank monitors incidents to establish patterns and possible connivance by agent's staff. 	Client (as with an outdoor ATM)
The agent's cashbox is robbed, or he is robbed on his way to/from the bank branch	<ul style="list-style-type: none"> Agent can keep smaller amounts of cash and travel more often to the branch. Bank can offer pooled insurance to all its agents. 	Agent
Identity theft		
Client shares or does not sufficiently protect his credentials	<ul style="list-style-type: none"> Require two-factor authentication (e.g., card plus PIN) Financial education by the bank 	Client (as with an ATM)
In a moment when the POS is unsupervised, someone uses it fraudulently	<ul style="list-style-type: none"> POS operators need to authenticate themselves with card plus PIN. Set defined session periods, after which operator needs to reauthenticate. POS only works with two cards and two PINs (operator and client), so securing POS alone is not enough. 	Agent
Errors or fraud relating to receipts		
Client's transaction does not match what is stated on the agent's receipt	<ul style="list-style-type: none"> Receipt is produced automatically by the POS device, with no manual intervention. Minimum content of receipt is specified by regulation (bank name, agent name, POS device ID, time and date, amount of transaction, etc.) Financial education: check the receipt. 	Client (as at a branch)
Transaction that appears to have failed (hence, no exchange of cash) did in fact go through.	<ul style="list-style-type: none"> Receipt is produced in all cases, even if transaction failed, to notify client of transaction status. Financial education: always get a receipt and check it before leaving. 	Client
Client is told printer is not working but is assured that he can still do the transaction.	<ul style="list-style-type: none"> POS device blocks automatically if there is no paper or printer malfunctions. Printer is placed within easy visibility of client, so he can see that one is being produced. 	Client (if he agrees to a nonreal time transaction)
Bank errors or fraud		
The receipt states successful transaction, but does not	<ul style="list-style-type: none"> Direct communication between POS at agent and bank's core systems. 	Bank

correspond to what happened in the client's account	<ul style="list-style-type: none"> • Proper controls on bank systems. 	
The receipt states successful transaction, but the value of the deposit subsequently disappears	<ul style="list-style-type: none"> • Standard bank regulation and supervision. • Deposit insurance for the client, if the bank ceases operations. 	Bank
Fraud by third parties		
POS device is stolen and used fraudulently	<ul style="list-style-type: none"> • POS must be used with card + PIN of authorized operator. For improper use, would also need a client card + PIN. • POS tied to communication point of agent (phone number, IP address). • POS automatically shut off by bank outside of agent's business hours. 	Bank
Client goes to a fraudulent agent, with a "fake" POS	<ul style="list-style-type: none"> • Bank could give a unique identification code to each client, and POS could show it prior to transacting so that clients can verify that they are 'talking' to the bank. • Clients should be able to easily check list of authorized agents from the bank or a public registry. 	Bank
The POS is manipulated (e.g., spyware is introduced)	<ul style="list-style-type: none"> • Use of specific-purpose terminals, avoiding open architectures. • Software can only be updated remotely with proper bank authorization. 	Bank
The communication between the POS and the bank is intercepted and manipulated	<ul style="list-style-type: none"> • All communications are encrypted end-to-end. • Appropriate level of security (e.g., at least 128-bit encryption keys). 	Bank