

Maintaining confidence in the system and protecting privacy

[Sociology](#), [Social Issues](#)



Confidence and trust in others is at the heart of the financial system.

Community confidence that the players in a financial system can securely store a customer's money and repay it on demand, make approved payments accurately and on time, and protect a customer's private personal and financial information.

Confidence in the system

In the predigital world, community and customers rely on largely well established players, licensed and subject to prudential regulation and supervision, while Digital technologies are leading to a rapid growth in the number of players participating in the payment process. Some of these offer an alternative to traditional systems, while others offer internal netting that allows the exchange of value between customer accounts within a digital business without recourse to the banking or payments system. However, as more sophisticated offerings emerge and customer usage begins to change, new risks will emerge and some existing risks will begin to shift to new players. To ensure community confidence is maintained in the financial system, policy makers will need to closely track new payment options and practices and the players that offer them.

The privacy of customer data

It is a principle for Banks that a customer's personal and private details must be protected. Unless required by law, most banks will not disclose customer data to a third party or use it other than for the purposes provided.

Digital financial services businesses encourage consumers to divulge bank account numbers, pins, and passwords to facilitate their operations. It is

often said, and increasingly true, that there is little or no privacy on the internet.

Trust in the safety of Banks and the Banking system

In the predigital world, banks regularly included images of their large below-ground vaults in advertising and designed their branches to look (and, in fact, be) physically strong and secure. Tellers were required to balance their cash at the end of every working day. Safety was focused on physical attack and the protection of cash, while now Cybersecurity is the largest security issue facing the financial system. These attacks involve a quite different set of perpetrators than banks are traditionally used to facing, including players with geopolitical as well as criminal objectives.

Bank Security

For the last two decades, cybersecurity in banks has been based on two central ideas—the creation of strong perimeter defenses (firewalls and similar mechanisms) and the encryption of data in transit outside the perimeter walls. More recently, increasing effort has also gone into monitoring system traffic and activity to identify anomalous events that might indicate fraud or attack.