SMART SECURITY FOR SMART DEVICES

The Better Way to Protect Digital Payments V.10

DISC HOLDINGS

rivetz

SMART SECURITY FOR SMART DEVICES

The Better Way to Protect Digital Payments

EXECUTIVE SUMMARY

Personal banking is the second most popular use of smart devices, only slightly behind on-line shopping. To allow customers to pay bills, check balances, or otherwise access their accounts, banks have always had to balance enabling convenience against risk and fraud. As systems move inexorably away from central core processing and in-person service to distributed architectures and app-based interactions, finding the right balance has never been more important.

> In the U.K., more than £500 million was lost to payment fraud in the first half of 2018 alone. The sophistication of cybercriminals' approaches shows no signs of slowing.

The costs of existing weaknesses already are large. In the U.K., more than £500 million was lost to payment fraud in the first half of 2018 alone. The increasing sophistication of cybercriminals' approaches shows no signs of slowing; most institutions see both the number and value of fraudulent transactions growing steadily.

Rivetz, in conjunction with its U.K. payments subsidiary DISC Holdings, is developing and offering a range of enhanced products and services designed to address the desire for convenience, trust and security among consumers without ignoring financial institutions' need to control risk and fraud.

CUSTOMER CONVENIENCE

Dealing with financial institutions has always been seen as complicated, compared with most other transactions. The reason is obvious – they look after customers' money, whether in physical or electronic form and criminals have always gone after the money. Recently, anti-money laundering rules and data protection requirements have been tightened by regulators, who have made it clearer than ever who is responsible for

identifying suspicious transactions. Those changes have placed additional burdens on banks, wealth managers, insurance companies and others, making it harder to open a new account; this adds cost and risk for banks, which they find difficult to pass on to customers.

> Changes have placed additional burdens on banks, wealth managers, insurance companies and others, making it harder to open a new account.

Passwords have remained the most popular way to control access and activity, because that method is familiar to most. Simple passwords aren't enough anymore, and other solutions have been piled on top, such as a series of security questions in the event of forgotten information or card security measures (secure token devices) taken at the time of an online payment to an unknown third party. All of this directly increases the cost to operate an account. At the same time, roughly one-quarter of all users have reported forgetting a password in the last six months. More than one-third fail to change their password more than once a year. The former requires extensive customer service interaction, while the latter increases the likelihood of theft. While the costs are indirect and spread across an entire business, they cannot be ignored at an institutional level.

While financial institutions are busy trying to prevent misuse of accounts, card companies now offer contactless payment cards, which offer no security protection in the event of a lost or stolen card. In an effort to manage risk, payments so far have been limited by a capped value (typically to less than $50 equivalent). Consumers and merchants like this approach, as it can shorten the payment time to 2 seconds or less. Volumes and values, even in relatively mature markets such as the U.K. have grown rapidly with the number of cards issued having doubled in only two years.

FRAUD IN PAYMENTS

Convenience comes at a cost. Losses are also rising fast and amount to $700 for every million spent of the value of all transactions. in the U.K. running at more than $3 billion per month, fraud is costing more than £2 million per month. Small retail operators pay a disproportionate amount of this cost.

Even so, contactless payments account for only a small fraction of overall payment fraud. A report from U.K. Finance suggested that in the first half of 2018, losses due to unauthorised transactions amounted to £358 million involving more than 1 million cases. Financial institutions prevented an additional £705 million of attempted fraudulent transactions.

Fraud fell into a number of different categories, such as type, location and means of access. Overall internet transactions accounted for by far the largest proportion by volumes and value. Numbers for mobile banking were comparatively small, but activity using these channels is also much lower and is relatively recent compared with online internet activity, which is now relatively mature.

Fraud remains a significant cost of doing business for almost all major financial institutions, wherever in the world they are located. Interestingly, a recent report from Experian suggests that most companies are happy to be 'competitive' in fraud detection and mitigation; only 35 percent have the ambition to be a leader. While many executives recognise the costs involved in allowing fraud to continue, they appear reluctant to incur the costs of more up-to-date techniques that might be used to reduce it. This includes the costs of a more intrusive security experience for the customer as well as the direct costs of the technology.

NEW APPROACHES

Rivetz is pioneering new approaches to security of devices. It is using its wholly owned UK payments subsidiary DISC Holdings to assess the applicability of these techniques to payments activity. Lessons learned will inform future development of capabilities that enhance both the user experience and also the ability of financial institutions to reduce risk.

EXAMPLE – STRONG CUSTOMER AUTHENTICATION FOR PAYMENT

Background

SCA comes into effect throughout the European Union in September 2019 as part of the new Payment Services Directive (PSD2). It is designed to offer consumers greater protection, particularly in the area of online commerce. It requires consumers and merchants to follow a two-factor authentication process, based on something the consumer knows (e.g. a password), something they are (e.g. a fingerprint) and something they own (e.g. a laptop or mobile device). At present, consumers typically are notified after the fact if money has been withdrawn from their account or a purchase made using a card. PSD2 requires that consumers give consent before the transaction is completed. This has caused merchants and others difficulty in terms of compliance and so implementation of this aspect of PSD2 has been delayed (most of PSD2 became effective in 2018).

Typical Approach

Most institutions appear to be solving the SCA issue by keeping the same core process but changing the flow. Consumers are being asked to receive some kind of one-time passcode, with a time-limited application. It's sent to either an email address or a mobile device via SMS. This passcode has to be typed into the application before the payment or change is enacted. This approach is not smooth, may require two separate devices and is prone to error. More importantly, it does not allow for any additional rules to be applied depending on the nature of the transaction – such as the value or nature of purchase. Nor does it allow validation of the integrity of the device(s) involved in the transaction.

The Rivetz & DISC Approach

Through integration of the Rivetz Confirm process with the DISC payment application, it becomes possible to not merely meet the basic requirements of PSD2 for SCA but rather surpass them. It enables:

- Proof that the devices in question were not compromised at the time of the transacation.
- A simple & seamless process of confirmation of a transaction before the fact.
- It enables policy with rules on keys - for example, if the payment is greater than a certain amount the device has to be in a specific location.

The approach therefore offers a better customer experience, is more secure and offers proof if the device has been compromised – to the benefit of consumer, merchant, bank and any other institution involved.

CONCLUSION

Provision of payment services involves risk. For financial institutions dealing with retail customers, balancing fraud risk and loss against the value of consumer convenience is a continuous process. In a climate of growing regulatory and cost burdens, experimenting with and investing in new ways of lowering risk cannot be undertaken lightly.

On the other hand, new payment methods now use devices that are themselves capable, if suitably programmed, of helping to reduce fraud. Rivetz enables solutions that can reduce risk, build customer trust, enhance the customer experience and drive out costs for the enterprise and service providers. By rolling out capabilities through the payment activities of DISC in the U.K., Rivetz intends to demonstrate the effectiveness of solutions in the real world, providing a simpler and safer experience.