MERCATUS CENTER
George Mason University

RESEARCH SUMMARY

A Chip Off the Old Block or a New Direction for Payment Card Security? Chips, PINs, and the Law and Economics of Payment Card Fraud

Consumer payments and data security have received a high level of public and regulatory interest as a result of a number of highly publicized data breaches at retailers such as Target, Michaels, and Home Depot. In response to security concerns, payment card networks in the United States have moved toward the rapid replacement of traditional magnetic-stripe payment card technology with new EMV computer chip–based technology (named for its founders, Europay, MasterCard, and Visa). The adoption of EMV-equipped cards came about as the result of private action, rather than by government intervention or mandate, through a "liability shift" that makes merchants or issuers who do not adopt EMV liable for losses due to fraud.

In "A Chip Off the Old Block or a New Direction for Payment Card Security? Chips, PINs, and the Law and Economics of Payment Card Fraud," law professors James C. Cooper and Todd J. Zywicki present an economic analysis of consumer payment cards regulation and payment card fraud that suggests the adoption of EMV was an efficient response to increased capabilities of fraudsters, and that mandated adoption of PIN verification likely would be socially wasteful.

KEY FINDINGS AND ANALYSIS

Payments card systems should not strive to attain zero fraud. Instead, they should strive to maximize consumer welfare by setting a level of security that optimizes the tradeoff between security and functionality. Eliminating all fraud would be cost-prohibitive in practice, harming consumers by dramatically reducing the value and usefulness of payment cards generally.

The optimal allocation of the cost and responsibility for payments security between networks and merchants will vary across societies and over time. For instance, in recent years, the speed and cost of a country's telecommunications technology has been an underlying factor determining the optimal allocation of payments security between networks and merchants.

- In the UK and Europe, where telecommunications technology has historically been slower and more expensive, the cost and responsibility of fraud prevention traditionally fell on merchants and consumers, because the payment might not be authorized or rejected until hours or days later. As a result, they developed the concept of chip and PIN as a substitute for real-time authorization.
- Countries such as the United States, where telecommunications technology historically has been fast and inexpensive, have been late adopters of higher-cost cards and increased POS verification methods by consumers and merchants (such as EMV chip). In the United States, better and cheaper telecommunications technology allowed for real-time online transaction authentication and sophisticated data analysis by processing networks.

For more information, contact Kate De Lanoy, 703-993-9677, kdelanoy@mercatus.gmu.edu

The United States' late adoption of the EMV standard and unwillingness to require PINs for customer verification likely does not reflect a market failure. The decision to create an incentive for EMV adoption but not PIN verification appears to be consistent with a desire to maximize the overall value of the system to all parties, taking into account the costs and benefits of greater security as well as the costs of alternative security precautions. What's more, effecting the movement to EMV through a liability shift likely harnessed private information on heterogeneous costs of adoption and risks of fraud.

Regulatory action to compel adoption of soon-to-be obsolete payments security technology, such as PIN-enabled cards and readers, will likely impose substantial cost with little or no long-term benefit to consumers. Issuers and networks are rapidly developing more secure and less expensive customer verification methods, such as Apple Pay, that improve security without PIN or other similarly high-friction verification technologies.

Lobbying by large merchants for mandatory PIN verification is not likely a response to a market failure. Larger merchants generally prefer that consumers use PIN debit rather than signature debit. The rationale has little to do with losses from lost/stolen cards since merchants that install EMV devices are not liable for lost/stolen fraud, the only source of fraud that PIN addresses. Instead, it more likely has to do with the savings merchants could realize if consumers were compelled to use PIN debit. The interchange fee for card payments is usually substantially lower for PIN debit than for signature debit, which is passed through to merchants in lower merchant discount rates for card transactions.

CONCLUSION

The consumer payment system has evolved spontaneously over time in light of available technology and efforts to reduce payments friction while also protecting consumers. Rather than blindly adopting the particular verification technology Europe put into place many years ago, US regulators should be alert to the evolving and contemporary nature of consumer payments and the fluid nature of threats to data privacy. Regulators should not freeze or hamper the adaptability of the payments system.