

Emerging Payments

Success depends on ability to control threats, misuse

Not long ago, criminals scammed hundreds of millions of dollars from Japanese pachinko parlors without ever cracking the security safeguards in place.

Instead, they worked around them.

The Japanese government and law enforcement officials designed a heavily encrypted, counterfeit-proof prepaid card for customers playing pachinko, a popular pinball-like slot machine. The cards were to be used instead of cash in an effort to curb tax evasion.

Rather than counterfeiting these cards, the fraudsters recycled used cards. Although hundreds were arrested in connection with the scam and thousands of phony cards were seized, the card sponsors' losses exceeded \$600 million. Clearly, it is a challenge to completely secure a system, especially with sizable amounts of money at stake.

"You can't anticipate every risk when

it comes to payments methods that are still emerging," says Rick Sullivan, a senior economist at the Federal Reserve Bank of Kansas City. "Fraud can infiltrate even a heavily encrypted system in unforeseen ways. But, confidence in these new payments products—and successful consumer adoption—depends on preventing misuse."

Sullivan, along with William Roberds of the Atlanta Federal Reserve Bank, and Jamie McAndrews and Michele Braun, both of the New York Federal Reserve Bank, recently authored a paper that focuses on risks associated with emerging payments methods. Their paper will be published in the New York Federal Reserve Bank's *Economic Policy Review*. As part of its mission, the Federal Reserve monitors payments methods, emerging methods and significant innovations.

The authors examined the risk issues associated with new payments types—which

in general have not been studied extensively—as well as alterations to established payments types.

“The predominant message is one of change,” Sullivan says.

Products, services, rules and technologies are all changing. So are the tools for perpetrating fraud and the techniques for mitigating them.

“Innovative payment mechanisms are making transactions cheaper and easier to carry out,” Sullivan says. “As with more traditional forms of payment, however, the ultimate success of these inventive arrangements will depend on—among many other things—their ability to control risk.”

Emerging payments and risks

In 2000, two foreign men tapped into Internet service providers in the United States to steal credit card, bank account and other financial information from more than 50,000 individuals, according to the U.S. Department of Justice.

The men then used that information to establish e-mail addresses and associated accounts at PayPal and eBay. They acted as both the seller and winning bidder in the online auctions, paying themselves with the stolen credit cards. Eventually, the FBI was able to lure them to the United States; they were sentenced to three years in prison.

This scheme is an example of data security risks involved as an unprecedented number of new payment types are being introduced.

New payment methods are based on existing payment products, with enhancements, innovations and rules added either to address new opportunities or take advantage of expanding technology. But, there isn't a precise definition of an “emerging payment,” or when a payment method becomes “established.”

Sullivan considers paper checks, pre-authorized automated clearinghouse (ACH) transactions, wire transfers, and credit and debit cards to be established payments, while those that differ (technologically, contractually, legally or conceptually) are considered

emerging. Examples include: general-purpose prepaid cards, PayPal, ACH payments initiated via telephone, and paper checks converted to ACH payments by billers and retailers.

Sullivan and his co-authors examined emerging payment methods that carry transactions relatively low in value and had a limited number of users during their start-up phases. These payment methods do not currently pose large-scale risks because of limited adoption in the early stage of their introduction.

“All payment processes introduce risks that need to be controlled,” Sullivan says, adding that fraudsters especially seem drawn to new technologies in an attempt to exploit early weaknesses, although they also attack established systems.

Sullivan and his co-authors explored the economic concept behind risks and propose a new framework for analyzing payment innovation. The types of risk most relevant, but not limited to, emerging retail payments are:

- **operational risk** (human or technical error that disrupts clearing or settlement),
- **fraud risk** (wrongful or criminal deception),
- **illicit use risk** (includes money laundering, terrorist financing, purchase of illegal goods and services), and
- **data security risk** (form of operational risk; unauthorized data use).

Emerging payments have special risk concerns for a few reasons. They are largely or wholly electronic, which can enable rapid proliferation of fraud and operational disruptions. Additionally, these risks must be almost nonexistent to ensure a new payment method succeeds.



It may require considerable effort and expense and definitely cooperation among all players to achieve.

The novelty of these payment methods implies various problems may not be anticipated and adequate safeguards may not be in place to address them.

“While not systemic (creating a domino effect), some risks associated with emerging payments are widespread and can disrupt aspects of general commerce,” Sullivan says. “Failure to address these risks may jeopardize viability. Experience shows that all successful payment systems have learned to keep most of these risks at fairly low levels.”

Managing risks

The amount of risk management depends crucially on the payment system participant who exerts the least effort. While this participant may determine the overall level of risk control, others with a lot at stake want a higher level of protection. This means some mechanism is necessary to give all participants the incentive to control risk.

“In general, market mechanisms seem to encourage the providers of a payment service to appropriately control their risks,” Sullivan says. “If providers fail to solve the problem, the business fails. But sometimes even this incentive is not enough.”

important role in reducing risk while monetary fines serve as deterrents.

For example, a large bank in the Midwest recently paid \$200,000 as part of a wider settlement for failure to perform due diligence on the legitimacy of customer activity.

In 2001, two companies’ telemarketing activities appeared to offer credit cards to consumers with poor credit records. The companies collected “membership fees” by having consumers read over the phone account information from their checks. The information was converted to electronic payments to the companies via the bank.

The credit cards were rarely, if ever, delivered, and customers were unknowingly signed up for other expensive programs. When customers called to complain, the companies used elaborate language to avoid repayment or cancelation. Eventually the companies were shut down and prosecuted.

The bank assisted the investigation and admitted its risk mitigation failure. For the first time, the Federal Trade Commission held a bank responsible for the deceptive practices of its customer. The bank agreed to vigorously screen prospective clients and monitor customer activities.

Mitigating risk in emerging payments has special concerns, Sullivan says. The methods’ newness implies various problems may not be

“ Only time and monitoring will reveal whether risk can be controlled sufficiently. ”

Service providers have three broad approaches to manage various risks: pricing, which means the party bearing the risk is compensated; insurance, or an agreement about who will bear the loss; and containment, which are activities that deter or suppress fraud.

Pricing and insurance alone are not sufficient techniques; containment is the dominant means of controlling risk in payments, Sullivan says. Vigilantly monitoring participants appears to be the most effective avenue to control fraud. Penalties also have an

anticipated, or adequate safeguards may not be in place. Emerging payment methods face a learning curve when confronting these types of problems, Sullivan says.

Participants’ privacy is tricky because every type of payment requires the exchange of some information. Therefore, every successful payment system has to reach a workable compromise between collecting users’ information and preventing misuse.

Competition provides an important incentive. Consumers’ selections reflects which

payment methods best facilitate smooth, low-risk transactions.

“Only time and monitoring will reveal whether risk can be controlled sufficiently,” Sullivan says.

Lessons learned

There are several key points for emerging payments methods to succeed:

- **Recognize the problem:** Features that add to the efficiency of new forms of payment—scalability, speed, anonymity—can also enable rapid proliferation of fraud. As information moves more easily among payment system participants, more intensive management is needed to safeguard data flow.

- **Maintain a perimeter:** All involved in legitimate payments (originators, receivers, banks, payment processors and networks) operate behind a protective barricade of security. Wrongdoers need to be kept out.

- **Trust the marketplace, but not blindly:** New payments products are immediately susceptible to operational, fraud and data security risks. Risk management responds to market incentives, though experience shows there’s a learning curve. At the same time, well-designed laws and regulations can help policymakers ensure the “public good” of confidence in the overall payment system.

“New payments products are likely exposed to fairly high levels of operational, fraud and reputation risk,” Sullivan says. “But, if a payment provider can address the problem quickly and effectively, it can stay in business. Containment is the dominant method to thwart these threats.”

Generally, market mechanisms appear to encourage providers to mitigate risks appropriately. Most providers, especially those in the private sector, have tools and incentives to manage many of these risks in part because they retain the option to exclude any party that fails to comply with a network’s safeguards. PayPal, for example, has learned through experience the techniques and tools to recognize risk and quickly correct it.



RICK SULLIVAN, a senior economist at the Federal Reserve Bank of Kansas City, partnered with other Federal Reserve colleagues to author a paper on risks associated with emerging payments methods. He shares their findings with peers.

The company manages fraud by denying or restricting access and blocking those who don’t comply with its rules. Its “verified” member program protects PayPal and creates a product that’s marketed to customers.

“With emerging payments, the problems, risks and gaps in processes can be addressed,” Sullivan says, “only if the providers and the participants apply constant vigilance as more and more payments methods emerge during this exciting time for the industry.”



BY BRYE STEEVES, SENIOR WRITER

FURTHER RESOURCES

“UNDERSTANDING RISK MANAGEMENT IN EMERGING RETAIL PAYMENTS”

By Michele Braun, Jamie McAndrews, William Roberds and Richard Sullivan
www.KansasCityFed.org/TEN

COMMENTS/QUESTIONS are welcome and should be sent to teneditors@kc.frb.org.