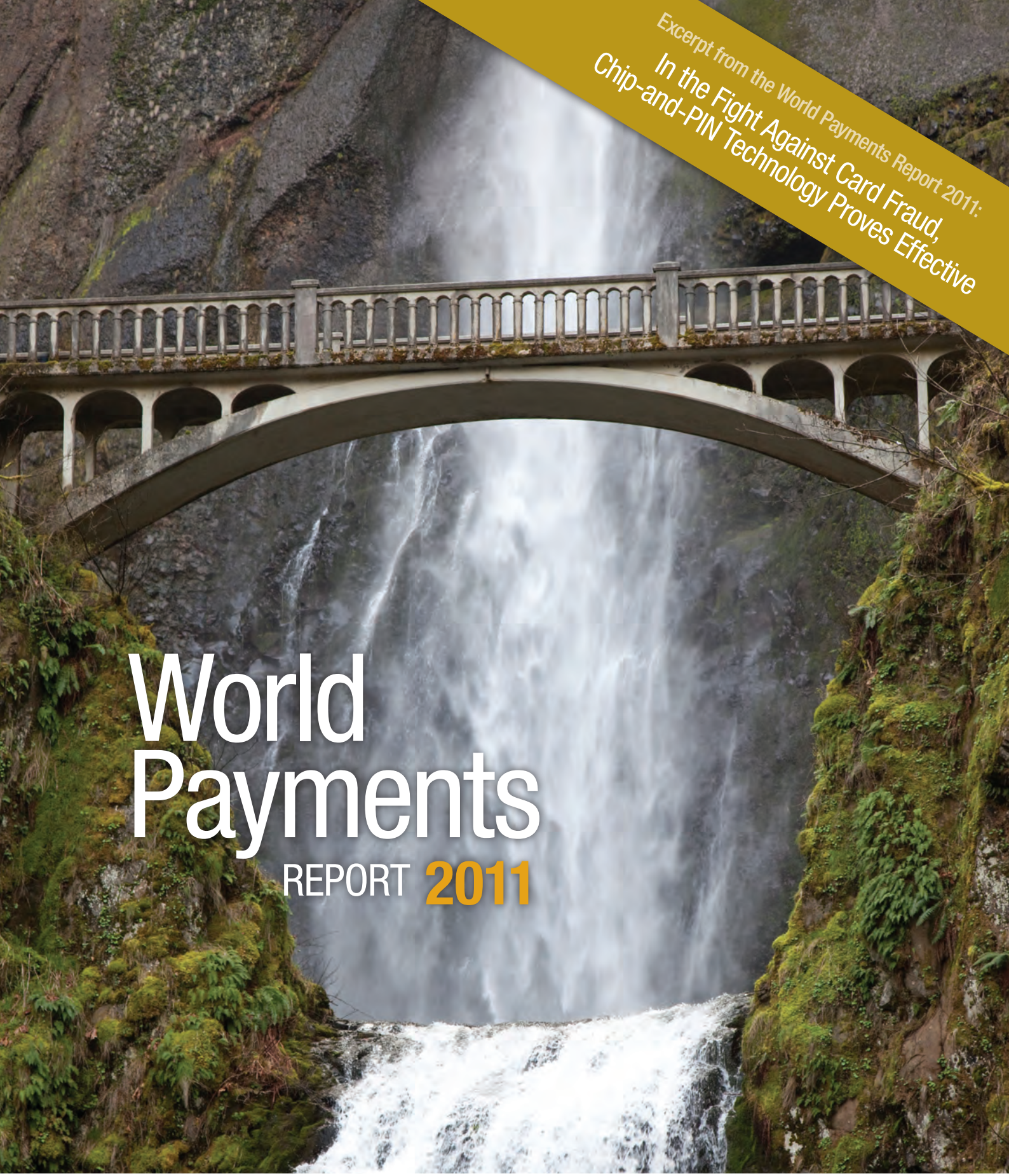


Excerpt from the World Payments Report 2011:

In the Fight Against Card Fraud, Chip-and-PIN Technology Proves Effective

World Payments REPORT 2011

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

RBS™

EFMA

SPOTLIGHT

In the Fight Against Card Fraud, Chip-and-PIN Technology Proves Effective

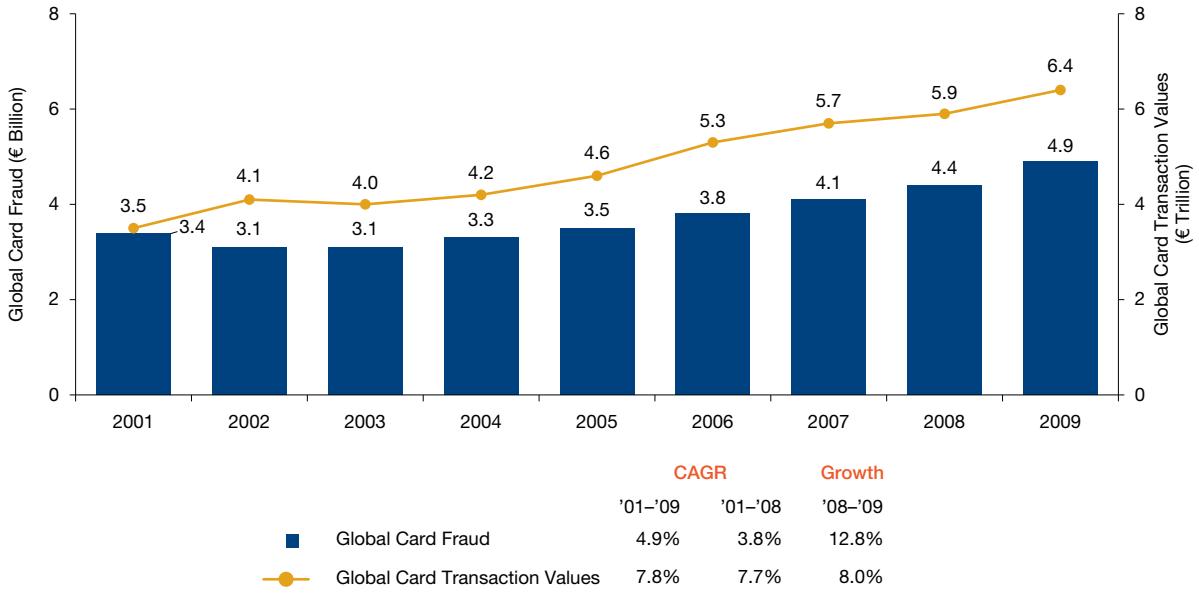
As the use of non-cash payments instruments grows, so does concern about the potential for fraud. The payments industry is pursuing various innovations to tackle fraud and better secure non-cash transactions—and thereby bolster consumer confidence. Attention is focused most, however, on e-commerce transactions, especially as electronic thefts increasingly hit the headlines.

Global card fraud has increased consistently along with card usage in recent years (see Figure 1.16). The number of fraudulent card transactions grew 7.2% and 12.8% respectively in 2008 and 2009, with the amount lost to card fraud totaling €4.9 billion in 2009, up from €4.4 billion in 2008 and €3.4 billion in 2001. As a result, the scale of card-fraud losses is growing as a percentage of total transaction values.

This rapid growth is largely because fraudsters have found more ways to compromise merchants' databases and processor data centers, gaining access to far more accounts than they could through traditional means such as stealing physical cards from wallets or mailboxes.

To help fight card fraud, many countries have moved toward chip technology, which has significant advantages over cards that only have magnetic stripes. Most notably, chips combined with a personal identification number (PIN) can generate dynamic data, producing a unique, one-time authentication for a specific transaction. This contrasts with "magstripe-only" cards, which use static data just to verify the card itself. The U.S. still uses mostly magstripe-only cards, but Europe and much of the rest of the world has or plans to transition to chip-and-PIN technologies, mostly using EuropayMastercardVisa (EMV) specifications that define the global interoperable standards for such cards.

Figure 1.16 Global Card Fraud (€ Billion) and Global Card Transaction Values (€ Trillion), 2001–2009

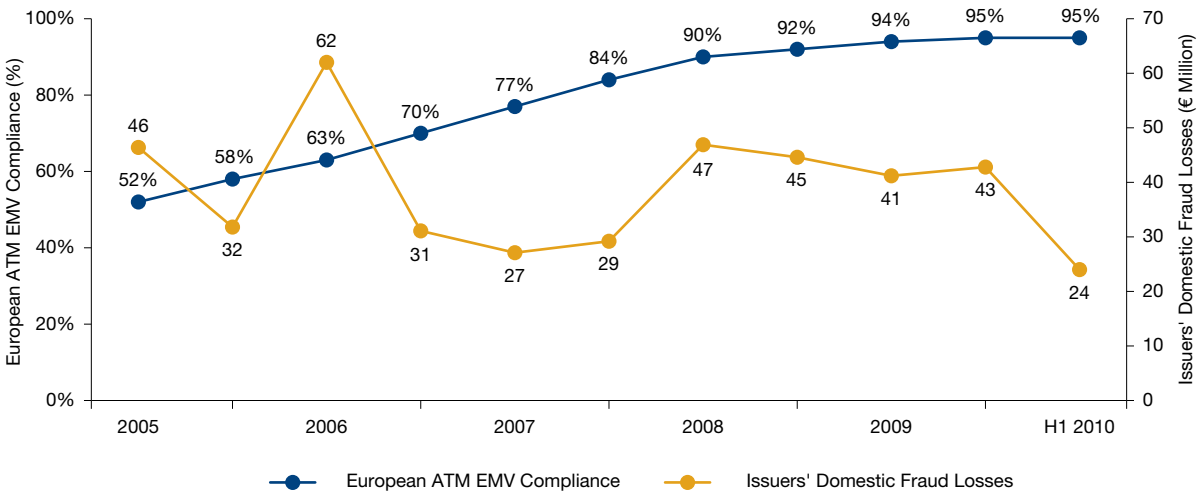


Source: Capgemini analysis, 2011

In fact, 95% of European ATMs are now EMV-compliant. Asia-Pacific has also witnessed growth in EMV-based smart cards, though adoption is greater in developed countries such as Japan and South Korea than in emerging markets such as India and China. EMV has proved highly effective in reducing fraud, especially related to face-to-face (POS) transactions, ATM withdrawals and lost and stolen cards. In the U.K., for example, counterfeit card fraud losses have dropped by 77% since 2004 when chip-and-PIN cards were first rolled out.[17] And across Europe, fraud losses have declined dramatically as more ATMs have become EMV-compliant (see Figure 1.17).

The U.S. is the single biggest exception in the global move toward EMV adoption. The U.S. employs sophisticated fraud-detection measures of its own, including real-time issuer authorization systems, but U.S. merchant groups and the Federal Reserve are nevertheless studying whether the growing vulnerability of magstripe cards warrants a shift to EMV-based chip-and-PIN cards. However, there would clearly be substantial costs involved in undertaking EMV implementation. EMV-compliant cards are more expensive to produce and issue than cards with a magnetic stripe, and switching to EMV would involve additional infrastructure and device costs.

Figure 1.17 European ATM EMV Compliance Rate (%) and European Card Issuers' Domestic Fraud Losses (€ Million), 2005–H1 2010



Source: Capgemini analysis, 2011; The European ATM Security Team (EAST): "European ATM Crime Report 2010"

[17] Financial Fraud Action U.K., "Fraud: The Facts, 2010".

In fact, a switch to EMV could cost the U.S. cards industry several billion dollars, making the business case complex; however there may be benefits beyond the simple reduction in existing fraud trends. At a systemic level, for instance, the U.S. will need to consider whether it could become an international magnet for credit-card theft if it keeps using cards that are easier to counterfeit. In addition, issuers and merchants will need to consider customer experience—as well as the potential loss of transaction volumes—if U.S. cardholders are unable to use their magstripe cards easily while traveling abroad.

CONCLUSION

At present, financial institutions and merchants are absorbing fraud-related costs, and significant investment continues to be made in fraud prevention solutions, using both tactical and strategic measures.

Technology and technical specifications are proving to be a critical tool in fighting fraud, and full global interoperability, most likely around EMV standards, could potentially prevent even more fraud from a variety of attack points within the payments system. This would position stakeholders to wage a more comprehensive fight on card fraud as a greater proportion of transactions become contactless and electronic.

The U.S. may or may not choose to follow the EMV route, but it seems likely that if EMV standards do continue to gain traction around the globe, fraud costs will increasingly shift toward non-compliant areas.