Avoid EMV Pitfalls

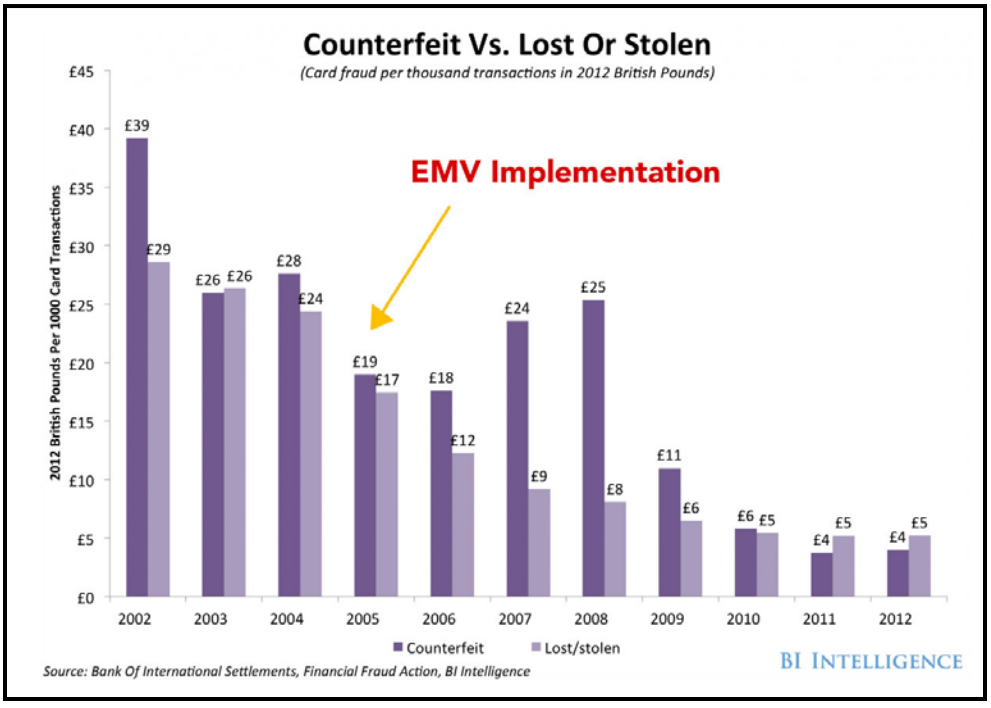
Save Time & Money with Clean Card Readers

CRIMINALS HAVE BEEN FINDING NEW AND INNOVATIVE WAYS TO COMMIT CARD fraud since Diner's Club introduced the concept in 1950. With well over 60 years of research and development, it should not be surprising to discover the traditional magnetic stripe system has been thoroughly outstripped.

Over the past two decades, card fraud has hit all-time highs – with counterfeit fraud occurrences and card-not-present (CNP) fraud gaining or exceeding losses from traditional lost or stolen methods.

While internet purchasing and CNP remain a fairly new issue, the networks implemented technology capable of directly addressing the issue of counterfeit card use – smart chip integration. Named after the companies who introduce it (Europay, MasterCard and Visa), EMV has been implemented worldwide – beginning with the United Kingdom in 2005 and working its way through Europe, Africa and the Middle East, Asia Pacific, Latin America, Mexico and Canada.

The UK began their EMV implementation in 2005. Throughout the first years of integration, they experienced a temporary increase in counterfeit fraud while criminals took advantage of the closing window. A good portion of the counterfeit fraud effecting UK credit and debit cards occurred in non-EMV compliant markets. Once EMV was well-integrated and card networks and issuers adjusted their acceptance requirements for foreign transactions, fraud saw a significant drop. Counterfeit fraud in the UK for 2015 was reported to remain around £43.4 million, according to a Payments Cards & Mobile report.

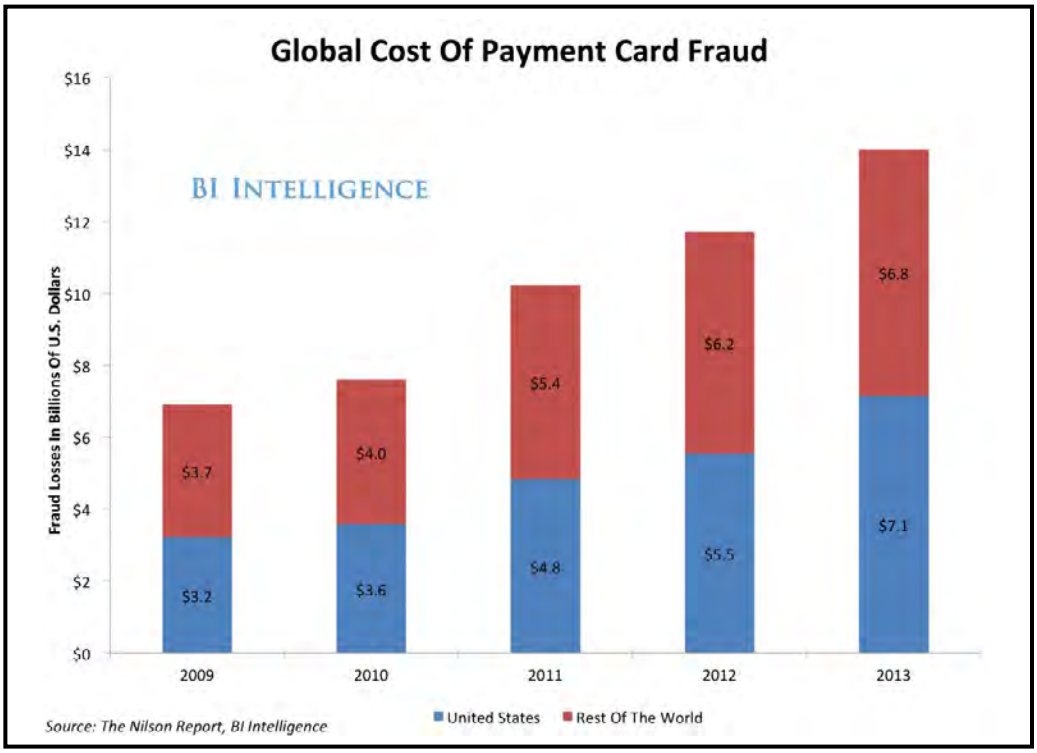


Card Fraud Over Time Source: BI Intelligence

Card Fraud in the United States

As other countries have made the transition to EMV, fraud has migrated to foreign markets (e.g. UK cards utilized in the U.S. and United States cards utilized in the UK). This migration has significantly boosted fraud in the U.S. – well beyond any regularly expected year-over-year trend.

According to The Nilson Report, a leading publication covering the credit card industry, counterfeit cards accounted for 49% of all card fraud losses worldwide in 2015. U.S. losses to counterfeiting jumped to $3.89 billion, accounting for 23.9% of global losses.



Global Cost of Payment Card Fraud Source: BI Intelligence

Counterfeit cards accounted for 49% of all card fraud losses worldwide in 2015. U.S. losses to counterfeiting jumped to $3.89 billion, accounting for 23.9% of global losses.

— The Nilson Report

What is EMV Fraud Liability?

The EMV liability shift in the U.S. is not a mandate. Instead, it has been set up as a program to encourage the payments industry to invest in chip card technology. Traditionally, fraudulent transactions – no matter the source – have been the responsibility of the card issuer or the network. Once the liability shifts take place, any counterfeit card fraud on a machine becomes the responsibility of the party in the transaction chain that lacks compliance.

For POS terminals, this liability shift took place on October 1, 2015. For ATMs, the transition begins on October 21, 2016 with the MasterCard network. All other networks implement their liability shift for ATMs in October 2017. Gas pumps are also subject to the October 2017 shift.

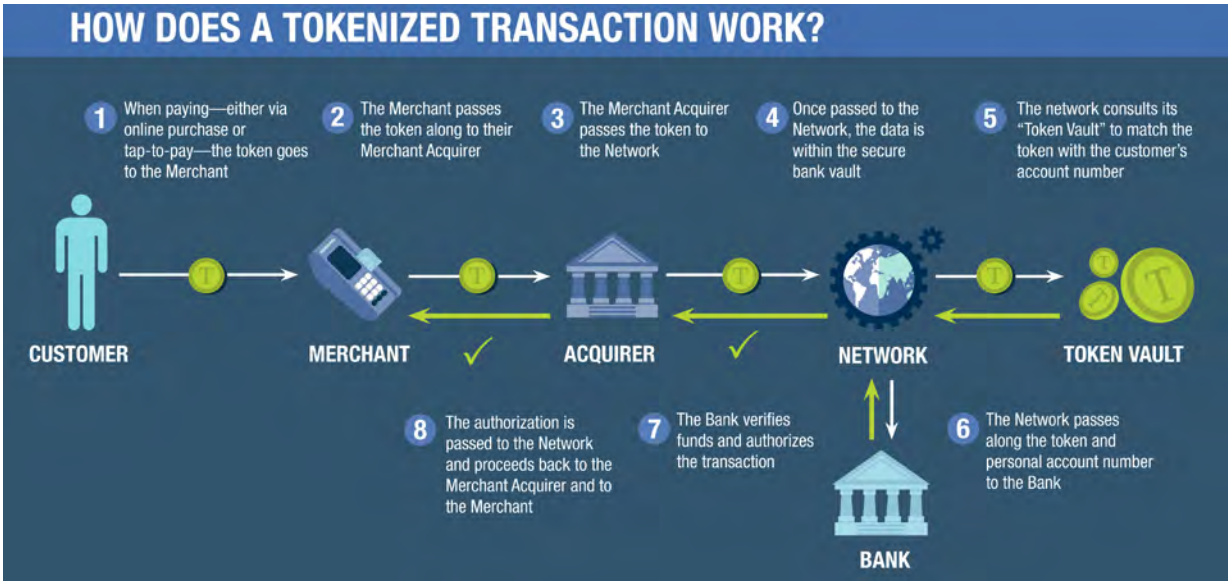
Data from the ATM Industry Association (ATMIA) and ATM manufacturer NCR estimate average costs of skimming to range $5,000 to $100,000 per incident – introducing a significant potential increase in operating costs for ATM operators.

The Mechanics of EMV Technology

The chip card technology utilized for EMV relies on a tokenization process to generate a unique and encrypted authorization process. When a chip-enabled card is inserted into an EMV compliant terminal, the terminal makes contact with the card to power the chip and initiate a transaction. The chip card then utilizes its internal programming to package the transaction information – merchant, cost, etc. – into a one-time use encrypted code to be forwarded through the payment processing system. The token must pass through the acquirer to the network, where the information is decrypted and bank authorization is sought. Authorization or denial is then sent back down the chain.

The tokenization technology used for EMV is designed around the idea of single-use codes, called "tokens." Counterfeit cards rely on the account information pulled from merchant transaction logs, copied from the front of the card or skimmed via magnetic stripe. This information is then duplicated onto a fake version of the card for use at POS, ATM and gas pump terminals. With EMV, each token is uniquely generated for a single transaction and any attempt to use the token for a separate transaction will result in a denial – rendering counterfeit cards useless.

Due to the tokenization and encryption process, EMV transactions require card contact and take longer than simple swipe transactions. "The first three months of EMV in the U.S. will be a learning curve for the ATM user, going from mag stripe to EMV chip. [ATM owners and operators should] enable latching on the EMV card readers to prevent customers using the new equipment incorrectly and prematurely removing their card before the chip has been fully read," said Bryant Lynch, manager, special projects for Access Cash based in Canada.



When EMV Fails

Just as with magnetic stripe, EMV card readers have their failures. Since EMV was deployed in Canada in 2007 on IMCRW card readers, "we have noticed an increase in card reader alerts," said Dimo Jovanov, senior manager, hardware & fraud, ATM channel for Royal Bank of Canada.

However, when EMV fails, ATMs are capable of defaulting to magnetic stripe data. This type of transaction is referred to as "Fallback." Depending on the ATM operator's agreement with their processor, it is possible for fallback to result in a higher transaction fee.

In addition to per transaction fees, a high level of fallback – at or above 7-10% of transaction volume – will raise red flags with the card networks. Networks then notify the acquirer, who has 30 days to address the issue. After those 30 days, the network reserves the right to introduce a fine – generally in the range of $25,000 per bank identification number.

When EMV fails, ATMs default to magnetic stripe data, which may result in a higher transaction fee depending on the processing agreement.

Device Malfunction

An EMV chip reader failure does not simply raise the costs on transactions. It also incurs extra costs for evaluation and repair. Depending on the maintenance service plan, this could be the price of a technician service call to the location – averaging between $100-600 per site visit – or be relegated to the time and costs for shipping and service of the equipment. Replacement card readers can run anywhere upwards of $200. These replacement and repair costs can add up fast.

Losing Transactions

Despite the additional costs, U.S. ATMs are currently somewhat protected from more significant losses by the ability to fall back to magnetic stripe. A failed EMV transaction does not currently result in a complete transaction failure. However, this may not always be the case.

Around four years ago, card issuers in the U.K. determined they would no longer accept non-EMV transactions. While balance inquires could be accommodated, no payments or cash dispense would be approved without chip encryption for card present transactions. Suddenly, a fallback to magnetic stripe was not an option. Clean, functioning EMV chip readers became essential in order to perform business. A malfunctioning terminal could mean a significant loss in revenue, especially for ATM operators with only a few machines.

An EMV chip reader failure does not simply raise the costs on transactions it also incurs extra costs for evaluation and repair — which can add up fast.

The Case for Proper Cleaning

"We have found that regular cleaning of the card readers is critical to ATM uptime," said Access Cash's Lynch. "Our experience has shown that the EMV chip contact degrades over time with contamination. This leads to transactions being intermittently declined by the host processor as the EMV data is incomplete."

Card readers are introduced to a large amount of oils, dirt and grime. These machines are encountering residue from consumer's cards as well as particles from the environment in which they operate. Restaurant machines are subject to additional grease, soaps and sugars. Convenience stores with gasoline operations may encounter an increase in gas or oil. Machines based outdoors, near roadways or in transit stations are subject to additional dirt, dust, water and other natural elements due to their proximity to the elements.

Cases of dirt, dust and bacteria impacting card reads are fairly significant. Terminal operators in the U.K. note levels of broken reader heads are far fewer than instances where card readers need cleaning. A 2013 study performed by NCR reported 78% of devices sent in for card read failures were merely dirty and were returned to service after being cleaned with a cleaning card.

In order to maintain proper transaction volumes and revenues, one prominent ATM operator in the U.K. has implemented maintenance zoning, providing techs specific territories where they are required to regularly inspect their ATMs, including frequent card reader cleaning.

"We have a cleaning arrangement as part of our preventative maintenance plan," said Suresh Nandihalli, COO of Euronet EFT EMEA business. "Cleaning of the card reader…helps to reduce service calls."

"Pre and post EMV, NCR proactively utilized its card reader cleaning kit to clean the card reader. This is carried out as part of any dispatch," Jovanov said. Regular cleaning of the card reader reduces downtime and malfunctions. "…this also applies to any type of card reader, not necessarily EMV."

Dirty EMV card readers can lead to:

- Increase in failed or fallback transactions
- Card reader errors and rejections
- Extended transaction times
- Customer frustration
- Poor customer experience

Reports from the field in Canada and Europe indicate regular cleaning of EMV card readers can impact up to 90% of reported fallbacks and device failures.

"Even though the ATM liability shift is just now taking place for the first card brand in the U.S., card reader reliability and the need for more frequent cleaning is a topic that has come up in our conference sessions and ATM deployer committee meetings," says David Tente, executive director of ATMIA U.S. and Latin America.

"Implementing EMV at retail ATMs in the U.S. requires both significant front end investment -- and a more rigorous ongoing maintenance regime to ensure ongoing EMV functionality," said Bruce Renard, executive director of NAC. "Part of the increased maintenance required with EMV involves regular card reader cleanings to remove excess dirt/oils/grime - to ensure that the more robust card information can be properly read/transmitted and fallback transactions avoided."

Industry experts agree exposure to elements and overall usage are significant factors in the break-down of card readers and recommend setting protocols or schedules to ensure regular cleaning.

Recommended cleaning schedules vary by location type and other influences such as the presence of food and drinks, weather and amount of use:

- **Indoor, low-use locations** – twice a month
- **Indoor, low-use locations where food is served** – once a week
- **Indoor, high-use location** – once or twice per week
- **Outdoor, low-use location** – twice per week
- **Outdoor, high-use location** – up to once a day

Avoid EMV Pitfalls

Malfunctioning EMV card readers are costly – leading to increased transaction charges and additional service and repair fees. However, the majority of faulty card readers do not truly need repair, they merely need to be properly cleaned. Implementing appropriate protocols or scheduling for regular card reader cleaning, utilizing low-cost cleaning cards, can significantly improve reader performance – resulting in fewer failed or fallback transactions, a decrease in errors, faster transaction times and greater customer satisfaction.

ATMIA

Established in 1997, the ATM Industry Association is a non-profit trade association with over 6,000 members in 66 countries. As an independent, non-profit trade association, ATMIA's mission is: to promote ATM convenience, growth and usage worldwide; to protect the ATM industry's assets, interests, good name and public trust; and to provide education, best practices, political voice and networking opportunities for members.