SAFE AND SECURE PAYMENTS: THE MASTERCARD APPROACH

Global point of view

For nearly 50 years MasterCard has been safeguarding the way you pay. We have been innovating solutions driven by data and insights to increase the safety and security of electronic payments.
Our safety and security guarantee:
we want to give consumers the peace of mind to pay with confidence, and our goal is to build a world beyond cash where every person, every payment and every device is protected.

Consumers need a safe and simple experience when making a payment, wherever they are in the world and whether they tap, click or swipe. MasterCard is investing time and money to continuously enhance the technology to detect and prevent fraud so that consumers can be confident that their money is safe.

In the rare event that fraud1 does occur, we ensure consumer peace of mind by limiting or eliminating cardholder liability2.

EXECUTIVE SUMMARY

MasterCard is the leading technology company delivering electronic payments and the leader in safety and security

- Technology and payment methods are changing every day – payments are becoming faster, smarter and more sophisticated.
- Cards remain one of the safest ways to pay, with only 6 cents for every $100 spent on major global cards lost to fraud. MasterCard’s safety and security measures have already reduced this number to 5 cents.
- We are investing in innovative payment and security solutions so consumers have a safe, secure and convenient payment experience.

Safety and security is our number one priority. MasterCard guarantees safety and security with smart technology to ensure we are always one step ahead of fraudsters

1. We are making sure consumers are protected from fraud before it even occurs
2. There is no silver bullet to fight fraud, and MasterCard has implemented multiple layers of protection to significantly reduce the risk of fraud:

- Unobtrusive network-wide tools help merchants and issuers identify and prevent fraud;
- New solutions and products in the consumer’s hand empower their transactions with the latest safety and security measures;
- Consumers are protected by limited / zero consumer liability guarantees for fraud, with efforts underway to expand this protection by working with local regulators, banks, and merchants;
- MasterCard led the initiatives on EMV (with chip-embedded cards its most visible hallmark) and SecureCode technology to dramatically reduce fraud;
- Our network screens 1.8bn transactions every month to help detect and eliminate suspect and fraudulent activity;
- We are already delivering data and insights to drive increased security across any device anywhere;
- We are testing voice, fingerprint and facial recognition identification innovations to keep payments safe.

---

1. It is important to keep in mind that fraud is separate from the compromise (i.e., exposure) of payment account information. Due to a variety of security measures implemented by the industry and MasterCard, only a fraction of compromises result in fraud, especially if the transaction requires authentication (i.e., verification).
2. As an example, all card transactions in the US are protected by our zero liability promise, eliminating financial exposure to the consumer in the event of fraud. MasterCard is working to extend this promise to other markets / regions.
KEY MESSAGES BY CONSTITUENT

Our overall message is: “We want to build a world beyond cash where every person, every payment, and every device is protected”.

CONSUMERS are ensured peace of mind against fraud

MERCHANDS are provided a rich ecosystem that rewards their efforts to prevent fraud by providing shifts in liability

ISSUERS are given sophisticated tools to improve their approval and fraud detection capabilities

MASTERCARD’S MULTI-LAYER PROTECTION

As payment methods and devices change and become commonplace in every aspect of our lives — whether stopping by a retail store in person or shopping online from a computer or a mobile device — MasterCard’s efforts have also evolved and adapted to ensure the safety of electronic payments wherever and whenever they occur.

Overall, authentication is the critical element of preventing fraud in both physical (Card Present) and non-physical (Card Not Present) environments and helps determine whether:

1. The card / payment device is genuine (card / device verification), and
2. The person initiating the transaction is the authorized user (cardholder verification).

While there is no silver bullet to completely stop fraud, applying a multi-layer approach that is coordinated across the industry helps reduce the risk of fraud significantly. EMV, SecureCode+, MasterCard Digital Enablement Service (MDES) and tokenization, as well as Risk Based Decisioning, are only a few examples of MasterCard’s broader efforts to fight the persistent threat of fraud, be it with card present or card not present payments.
MasterCard leverages the power of its network to monitor transactions across the globe and identify fraud. **EMS (EXPERT MONITORING SOLUTIONS) and FRM (FRAUD RULES MANAGER)** are at the core of MasterCard’s anti-fraud efforts, underpinning our ability to detect suspicious activity and transactions and provide issuers with the tools to supplement their own fraud systems and processes.

MasterCard company DataCash also offers **GateKeeper:2.0**, an advanced fraud and risk management solution, for merchants to keep chargebacks to a minimum whilst protecting genuine customers. The solution uses layers of sophisticated technologies, such as expertly crafted rules, shared databases, device ID, etc, to precisely identify a transaction’s level of risk. High risk transactions are automatically rejected whilst low risk transactions are accepted. A small number of transactions that are not clearly fraudulent or genuine can be manually reviewed via an intuitive user interface which enables further analysis for a more informed decision. The solution is differentiated by a team of experts that have vast experience of fraud trends across multiple industries and achieves industry leading results.

MasterCard – in partnership with Visa, American Express, JCB, and China UnionPay – developed and implemented the **EMV specification, with the chip payment method** its most visible hallmark. MasterCard has introduced the M/Chip and M/Chip Advance payment applications to secure our payments globally. The embedded chip on the plastic card along with the MasterCard payment application is significantly more secure than magnetic stripe cards and its introduction has reduced counterfeit fraud by 60-80%.

**Fraud losses (CAD $mm) Fraud as bps of spend**

<table>
<thead>
<tr>
<th>Year</th>
<th>Fraud losses (CAD $mm)</th>
<th>Fraud as bps of spend</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>$95</td>
<td>6.3</td>
</tr>
<tr>
<td>2007</td>
<td>$107</td>
<td>6.8</td>
</tr>
<tr>
<td>2008</td>
<td>$109</td>
<td>6.2</td>
</tr>
<tr>
<td>2009</td>
<td>$142</td>
<td>8.3</td>
</tr>
<tr>
<td>2010</td>
<td>$119</td>
<td>6.8</td>
</tr>
<tr>
<td>2011</td>
<td>$70</td>
<td>3.8</td>
</tr>
<tr>
<td>2012</td>
<td>$39</td>
<td>2.0</td>
</tr>
</tbody>
</table>

**EMV Timeline**

- EMV piloted in Canada
- EMV launched – liability shift and implementation

73% drop in fraud dollars

In Canada, where **Chip and PIN is commonplace** (90%+ penetration), fraud declined 73% over 4 years, falling from $142 million in 2009 to only $39 million by 2012 (2.0 bps of domestic debit card volume).

MasterCard continues to push for global adoption of EMV and has led efforts to encourage a fraud liability shift by late 2015 in the US, the last major market to withhold from widespread acceptance.
MasterCard Digital Enablement Service (MDES) will introduce a new secure platform for payments via mobile devices, including both Card Present and Card Not Present environments by late 2014. MDES substitutes the real card number with a "token" account number. This token is "translated" back to the real account number by MasterCard at the time of purchase, so the issuer can match up the transaction with the correct account. If compromised, tokens cannot be used by fraudsters to facilitate fraud. As an added benefit, the merchant only receives the token and never sees real account data, removing a further point of weakness for fraudsters to target.

In 2013, MasterCard launched SecureCode+, the latest upgrade to its SecureCode technology, which allows merchants to add another layer of security for online transactions by asking the consumer to enter a password using SecureCode+. The SecureCode+ password is only known by the account owner and the merchant can choose which transactions are required to use it. Merchants do not have to use SecureCode+ if they trust the transaction and can dial their authentication needs up or down depending on the desire for further verification.

SecureCode+ can also provide a liability shift for merchants: The more a merchant attempts to protect the end consumer through authentication, the more they benefit from protection against fraud.

In 2013, SecureCode authenticated 1.4 billion transactions globally, reporting 28% growth in a single year. By dollar volume, SecureCode ensured the safety of about 29% of all online spend around the world.

Risk Based Decisioning will add a third layer of security in the CNP space. Its basic premise is to use a consumer email address, device information, and account number to develop a unique online “persona.” Based on this digital footprint, we can seamlessly authenticate consumers with no effort on their part. Over time, this unique persona will be given a reputation score which can be used by merchants and issuers with their payment approval process.

As an example, returning consumers with a high reputation score can proceed through checkout without ever having to authenticate, resulting in a faster sale with higher likelihood of satisfaction and fewer abandoned purchases.

Our Top Priority: Safety and Security for Consumers

In the event fraud occurs, we ensure the consumer is partly or wholly shielded from financial liability or loss resulting from fraud. Consumer liability is generally determined by local regulatory conditions, and MasterCard is working with governments around the world to ensure our rules are one step ahead when it comes to protecting consumers. From a merchant and issuer perspective, the rules for determining fraud liability are complex and varied, but are aligned to reward the party that exerts the most effort to secure the transaction.

Our Promise to Protect the Consumer from Fraud Will Remain Our Utmost Priority.

MasterCard leverages our brand, reputation, and franchise to shield consumers from fraud. Our efforts have already reduced cardholder liability around the world, and in the US we have managed to establish a zero liability guarantee. We aim to expand this zero liability guarantee to our cardholders globally and continue to work with local regulators, banks and merchants around the world to protect the consumer.
**APPENDIX**

**FRAUD 101**

*Fraud is the financial loss associated with unauthorized use of an account*, whether it is using those credentials to buy merchandise, transfer funds, withdraw money, or receive some other financial benefit.

Consumers place safety and security as their first and foremost practical and emotional need for their payments. Credit and debit cards have gained prominence and ubiquity as financial instruments due to their ability to satisfy these needs.

In 2012, it was estimated that US credit and debit cards experienced approximately 6 bps of fraud, and MasterCard leads the industry with an even lower figure (5 bps).

**THE COST OF FRAUD**

*The US comprises 45% of global fraud, but only 24% of global spend. Card Not Present comprises 45% of global fraud, but only 8% of global spend. Card Not Present fraud is still 3x greater than Card Present, despite being declined 6x more often.*

Fraud cost the global card industry more than USD $11 billion in 2012. Despite making up less than a quarter (24%) of the world’s payments volume, the United States constitutes almost half (47%) of all fraud losses, losing $5.3 billion to criminals. The fast-growing online retail space is a particular challenge. Despite being screened and declined almost 6x as often as Card Present (CP), Card Not Present (CNP) fraud is 3x higher.

![Diagram showing the cost of fraud](image-url)

Source: MasterCard data warehouse, 2013

Source: Nilson Report 2013, MasterCard data warehouse; last 12 months figure is through 3Q 2013. All cards (global) figure includes MasterCard, Visa, American Express, China Union Pay, Diners Club, and JCB.
For card fraud to occur, the perpetrator must successfully navigate a few major barriers:

1. Payment account information is lost, stolen, or otherwise compromised and
2. The issuer authorizes the transaction as a legitimate purchase.
3. In some cases, the perpetrator may also be required to authenticate (i.e., prove they are the legitimate cardholder).

In other words, the perpetrator must find a way to obtain account data and then successfully imitate the legitimate user’s typical purchase behavior when attempting to consummate a fraudulent transaction.

The authorization and authentication steps are unique to cards and, as a result, only a small percentage of compromises of account data lead to fraud.

ILLUSTRATIVE OVERVIEW OF CARD FRAUD PROCESS
FRAUD PROTECTION IN PRACTICE: TWO CASE STUDIES

To illustrate the points discussed in this paper, we present two sample case studies: (1) a phishing attack to expose data which is later used to make purchases online and (2) the theft of data from a payment system to sell account information and produce counterfeit cards.

FRAUD CASE STUDY #1: PHISHING COMPROMISE, CARD NOT PRESENT PROTECTIONS

1. Consumers receives email purporting to be from a trusted source (e.g., friend, reputable company etc.) asking consumer to click on the link.

2. Clicking the link installs malware or uses social engineering to trick consumer into revealing card account data.

3. Informations is used to make online purchases or cline cards. With SecureCode+, however, accounts are protected by the consumer’s secure password.

While not technically sophisticated, phishing compromises are difficult to protect against given the consumer is often the party disclosing account information. Nonetheless, innovations such as SecureCode+ will make it much harder for fraudsters to perpetrate their activities online.
**FRAUD CASE STUDY #2: DATA BREACH COMPROMISE, CARD PRESENT PROTECTIONS**

**ILLUSTRATIVE EXAMPLE**

<table>
<thead>
<tr>
<th>Data compromise activities</th>
<th>Fraud protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Perpetrators access retailer's system through compromised admin credentials (e.g. obtained through brute force, phishing, etc.)</td>
<td>• Terminals only capture the data required to process a transaction – E.g. without CV2, online/CNP fraud is difficult to commit</td>
</tr>
<tr>
<td>• Malware installed in the POS environment to capture card data; when swiped, card shares data with the POS</td>
<td>• Issuers, acquirers, and merchants can monitor for suspicious activity</td>
</tr>
<tr>
<td>• However, data is stored or transmitted in clear text in the POS environment, and in some cases is encrypted too late in the process</td>
<td>• MasterCard can inform issuers if point of compromise is known; issuers can decide which accounts to close and reissue vs. keep open and monitor</td>
</tr>
<tr>
<td>• Data is now vulnerable to capture by the malware</td>
<td>• In the event of fraud, consumers are covered in part or in full depending on local market rules and regulations</td>
</tr>
<tr>
<td>• Account data sold through online black markets or directly used to attempt fraudulent purchases</td>
<td>• If EMV had been present, cloning the chip would be extremely difficult and its use of a dynamic secure feature would make it nearly impossible to &quot;replay&quot; transactions</td>
</tr>
</tbody>
</table>

While targeting a retailer’s systems can yield millions of accounts, protections put in place by the card industry and MasterCard can effectively close down more than 90% of attempts at fraud, with even lower actual financial loss. The EMV chip and its dynamic capabilities would have made it harder for fraudsters to clone cards. In addition, new developments such as MDES and tokenization would have yielded tokens instead of real account numbers, further protecting consumers and merchants from fraudsters.

However, while direct fraud costs may be relatively low, the full effects of the compromise are very serious, including the loss of confidence in the payments ecosystem, lost sales at the retailer, negative impacts on brand and reputation, and so on. While infrequent, a single major event can cost a retailer upward of $100 million in direct losses, not including other negative effects such as a drop in market capitalization / stock prices.