MAGENSA™

SIMPLY STOPS FRAUD

The Heart of Magensa's Credential Authentication Service

MagnePrint®: A Real Time Risk Management Tool

☎ Call a representative to learn more 562-546-6500.

Introduction

There are several technologies that underlay all the fraud prevention, detection and advisory services offered by Magensa. When card credentials are involved, the first is cryptography and the second, but more important component, is MagnePrint. The MagnePrint risk management tool allows Magensa to provide the Payment Card Industry (PCI) with an additional layer of protection against fraud, in card-present credit, debit and ATM transactions. The purpose of this paper is to explain to a technically informed audience the tool, the technology and processes behind it, and the benefits that will accrue from the use of MagnePrint to issuers, processors, acquirers, merchants, brands and consumers.

Important components to prevent fraud: cryptography and more important, is **MagnePrint.**

MagnePrint is a dynamic card authentication technology based on the unique physical properties of the magnetic stripe, also referred to as the stripe's digital identifier or (DI). It provides validation that the card itself is genuine and that its encoded data has not been altered. The MagnePrint risk management tool, developed by MagTek, Inc., and licensed to Magensa, imposes no significant time cost and only a minimal dollar cost on the merchant at the point of transaction. The necessary infrastructure investment is negligible in the context of the ongoing costs of fraud to issuers, processors and acquirers.

Additionally, its success does not depend on a mass re-issuance of cards, since the cards currently in circulation can be brought into participation over time in the course of their normal use.

fraud

$4.6B

worldwide loss in credit card fraud.

▼

save

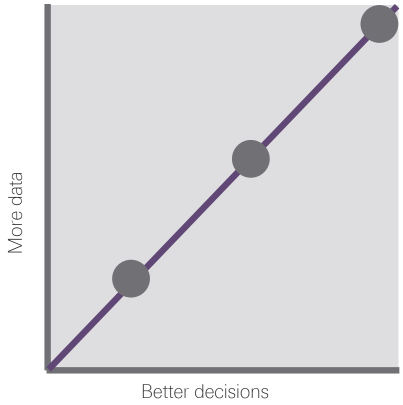
$2B

We can cut that number almost in half.

MagnePrint technology is complementary to chip technology. For the foreseeable future, the magnetic stripe will remain as either the primary or fall-back machine-readable technology on financial transaction cards. The chip will not protect the magnetic stripe, but MagnePrint will. Additionally, the chip too can be protected against cloning by MagnePrint. This is true because chip cards today are protected solely by sound key management processes. If the process breaks down, chip cards can be cloned quite readily. The chips are small man-made computers embedded in the plastic. They have no inherent unique biometric feature. If you can make one, it can be copied. MagnePrint is a naturally occurring phenomenon, not a man-made process. Used in conjunction with a chip card, it can provide evidence that the chip card has not been altered or cloned - post production.

Worldwide, reported credit card fraud is an annual U.S. $4.6 billion problem, with an unknown but likely significant additional cost related to unreported debit and ATM card fraud. Credit, debit and ATM card fraud is everyone's problem. The costs of fraud are carried initially by issuers and acquirers, who pass them on to merchants in the form of authorization fees and discounts; merchants then pass them on to consumers in the form of higher prices for goods and services.

Over time, we anticipate the adoption of MagnePrint technology will lead to an annual savings in the range of U.S. $2 billion of card-present credit card fraud. In addition, there will be annual savings directly related to the elimination of currently unreported debit card and ATM fraud. Furthermore, online internet transactions will be protected by consumer use of portable, MagneSafe Secure Card Reader Authenticators (SCRAs) that feature MagnePrint. The payment and identification world will shift from "card present" to "authentic card present".



More data, better decisions: It's empirically clear that the current authorization system is generally successful in keeping credit card fraud within a predictable, actuarially useful range. But the system is not perfect. As noted above, in the range of U.S. $4.6 billion worth of fraudulent transactions are cleared per year, the vast majority of which presumably represent "false positives" that were erroneously approved by the authorization system.

No matter how much information is available, the decision to authorize a given transaction (to indemnify the merchant for that transaction, provided that certain conditions are met) is always a statistical judgment call -- a risk-management decision. The authorizing party adjusts its authorization algorithm to take into account all available, relevant, information and the algorithm produces an authorization decision.

The accuracy of that decision, and its effectiveness in filtering out fraud, is directly related to the amount of information available to the algorithm. More data yields better decisions. For example, if the payer's identity and the card he presents were authenticated at the time of transaction, it would without question reduce the incidence of fraud.

It was in the spirit of "more data yields better decisions" that the MagnePrint risk management tool was developed. MagnePrint is a way of providing another useful, reliable piece of data about the likelihood that a given credit, debit or ATM card is authentic.

MagnePrint Identifies the original: MagnePrint uses the inherent properties of the magnetic media to provide the authorization algorithm with a reliable means to assess the cards originality. It indicates if the card presented is the original card delivered by the issuer -- not a clone, not a copy, not one that contains altered data on the magnetic stripe, but is the unique original card.

There currently exists no other cost effective technology capable of providing such statistically reliable, real time authentication of the payment instrument in a credit, debit or ATM card transaction. As a result, those that take MagnePrint into account in the authorization process should see an immediate and material decline in counterfeit card fraud losses.

No two cards are alike.
Stochastic nature of magstripes.

MagnePrint Fundamentals

54

bytes of data

What is MagnePrint? This technology was developed to generate a numeric value that could serve as the digital fingerprint of a specific magnetic stripe credit or debit card. This digital fingerprint, known as a MagnePrint, is a value that is determined automatically when a card is read in a MagneSafe Secure Card Reader Authenticator (SCRA) that features MagnePrint.

How is the MagnePrint value determined? MagnePrint technology, based on research conducted by Washington University's Department of Security Technologies, measures the background magnetic particulate distribution on a standard magnetic stripe card, and converts that distribution into a 54-byte value that is a simplified representation of that particulate distribution.

What needs to change on the current card? No changes are required to the manufacturing process of the magnetic stripe, the plastic card manufacturing process or the data encoded on the magnetic stripe. Also, there is no need to re-issue cards.

Why is MagnePrint useful? Because the particulate distribution is persistent over the useful life of the card, multiple MagnePrint values read at different times from the same physical card, provided the encoded card data has not been changed, will always be equivalent within statistical limits.

In contrast, the MagnePrint values read from different physical cards, even if encoded with identical card data, will always be different. This means that the MagnePrint serves as a reliable indicator of the identity of a physical card, and can be used to prevent the authorization of fraudulent card-present transactions initiated from cloned, skimmed or altered cards.

How does MagnePrint recognize potentially fraudulent transactions? When a card-present transaction is submitted from a MagnePrint-enabled reader for authentication at Magensa or another MagnePrint-enabled host system, the MagnePrint of the card read at the transaction point is transmitted along with the card data and other data.

The MagnePrint risk management tool compares the transaction MagnePrint value to a reference MagnePrint value already present in the authorization database, calculates the degree of correspondence (the match value) between the two values, and makes a judgment about the card's authenticity based on all available transaction information, including the match value.

What technology is required? The MagnePrint risk management tool requires a MagneSafe Secure Card Reader Authenticator (SCRA), which features MagnePrint, at the point of transaction, and ability for the merchant, processor, acquirer or issuer to transport the MagnePrint values to the Magensa Registry or another MagnePrint enabled Host. The MagnePrint-enabled components can be retrofitted into most existing card authorization systems.

Four layers of security

MagnePrint technology offers four layers of security. These are increasingly impregnable layers that act as barriers to prevent the compromise of MagnePrint technology.

01

Complexity The first layer is inherent in the complexity of the particulate distribution on a standard magnetic stripe. The MagnePrint algorithm leverages the fact that the 3.375 inches of stripe space along each card's encoding area are populated by a persistent random distribution of particles that are permanently fixed. Changes in the magnetic stripe's physical structure that occur during a card's lifetime, e.g., by abrasion during normal use, are statistically insignificant.

The likelihood that two different cards will yield identical particle distributions, given the randomness inherent in the process by which magnetic stripes are manufactured, is in the range of one in 900 million. And the hundreds of millions of particles make it statistically and practically impossible for an existing magnetic stripe to be cloned with a particle distribution pattern that will yield an equivalent MagnePrint value.

02

Pattern As a second layer, MagnePrint technology determines the 54-byte MagnePrint value in reference to the positions of the flux reversals of the encoded card data. The data pattern is larger, by orders of magnitude, than the particle pattern. Therefore, if a valid card with a known particle pattern were to be re-encoded with identical data, it would show non-trivial variances in the way the encoded data pattern microscopically aligns with the physically permanent particle structures of the magnetic stripe on the card. As a result, cards with altered data can be detected with MagnePrint technology.

03

Random The random variations inherent in each incidence of reading a card offer a third layer of security. Each read of a card, whether the card is swiped by hand, or inserted into a motorized or dip reader, is a stochastic process. Due to the principle of entropy and certain factors of imprecision such as swipe speed, pressure, direction, acceleration and reader to reader variations, the MagnePrint will change unpredictably with each swipe but within boundaries that allow it to be measured and validated.

Paradoxically, this means that a transaction MagnePrint value that is identical to a previous MagnePrint value on file is almost certainly fraudulent and will be rejected by Magensa. Multiple MagnePrint values taken from the same card on successive reads are expected to vary, within a statistical range. The probability of an exact match on all 54 bytes in separate card reads is in the range of one in 100 million. This inherent variability provides a statistically probable, unique transaction value for every card swipe, adding far greater security to the payment system and reducing the value of card data obtained through criminal cardholder database breaches.

04

Plain View Finally, as a fourth security level, the MagnePrint authorization process is protected against fraud by the simple fact that it depends on information that is in plain view. There is nothing hidden about the particulate structure of the card or the encoded alphanumeric data. This means that there is no "secret" to the fundamental MagnePrint technology that, if cracked, would compromise the system.

0.027%

false reject rate

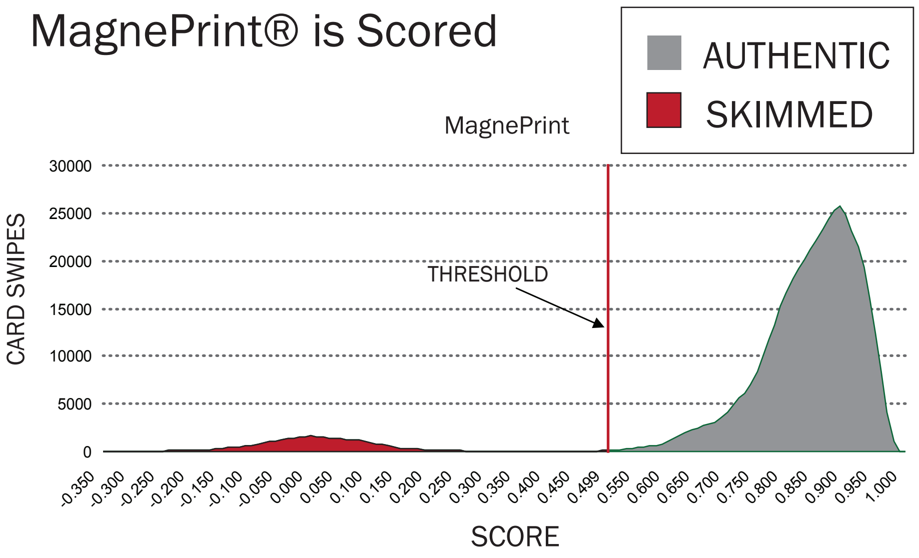
Determining acceptance criteria: It is important to understand that MagnePrint does not guarantee the authenticity of the transaction. It provides the card acceptor or authorizer a data point representing the probability that a given card used for a transaction is authentic. By using this data point, a card acceptor or issuer can establish an acceptance criterion for a financially acceptable level of risk.

During one test of MagnePrint, a run of a million transactions with an acceptance threshold set at 0.5 resulted in a "false accept" rate of zero, that is all attempts to process fraudulent cards were thwarted, and the resulting "false reject" rate was only 0.027 percent.

In comparing a given transaction MagnePrint to its reference MagnePrint, the scoring algorithm assigns a match value between zero (no match) and one (perfect match). The MagnePrint authorization methodology allows each relying party to select an acceptance threshold between zero and one for its transactions, or even to specify a threshold that varies according to the characteristics of the transaction (e.g., more stringent for higher-dollar transactions originating from a fraud prone merchant).

As important as it is to reject fraudulent transactions, for many merchants it is just as important not to reject legitimate transactions (i.e., not to generate "false rejects"). In order to preserve customer goodwill, some parties might wish to be more forgiving, e.g., set the acceptance threshold at 0.35, which would result in authorizing a very small number of fraudulent transactions while statistically eliminating the incidence of "false rejects" and still maintaining the robustness of MagnePrint as a risk management tool.

These risk management decisions have been deliberately left in the hands of the relying party, so that each can establish acceptance thresholds that are prudent in the context of its own business and its own customers.



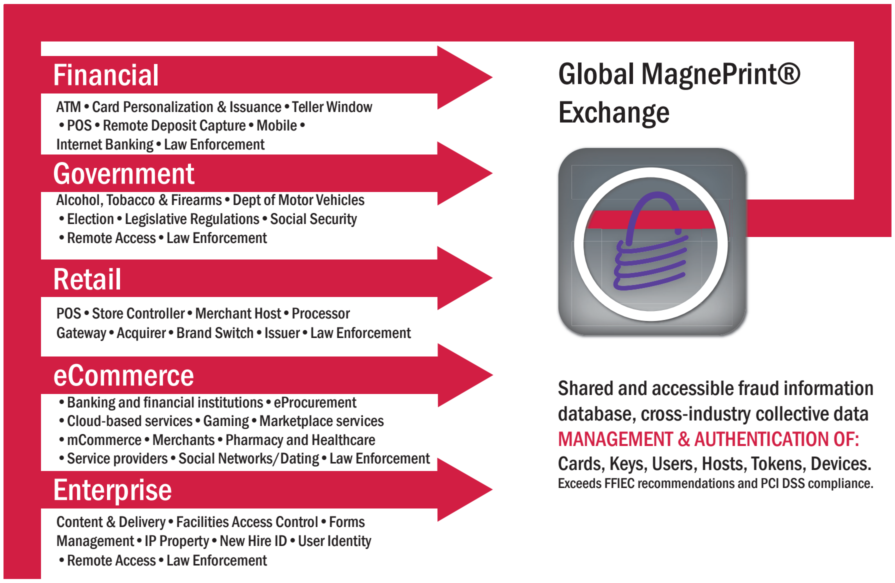
Growing the Magensa MagnePrint Registry: The MagnePrint risk management tool depends upon the presence of a reference MagnePrint in the authentication database. This allows correlation of the transaction MagnePrint data and the reference MagnePrint data to authenticate the card.

Reference MagnePrint data should be collected as a matter of course whenever a card's identity is known with certainty, e.g., at the time of issuance. To avoid re-issuance costs, however, reference MagnePrint data can be gathered on cards already in circulation without imposing an unacceptable inconvenience on cardholders.

When a transaction MagnePrint is submitted as part of the authorization data set, and if no reference MagnePrint exists for that card, this first transaction MagnePrint is presumed to be legitimate and recorded in the Magensa authentication database with "provisional" status. Henceforth, the provisional MagnePrint collected at the time of this earlier transaction will be available for use as the reference MagnePrint in authorizing future transactions.

The authenticity of this provisional MagnePrint is not guaranteed, because it was collected in circumstances in which the authenticity of the card from which it was provided was not known with 100 percent certainty. However, there is a strong statistical probability (inherent in the overwhelming margin by which legitimate transactions outnumber fraud attempts) that any such "provisional" MagnePrint will be legitimate, so treating all such provisional MagnePrints as authoritative, in the absence of evidence to the contrary, is a statistically rational business decision.

Furthermore, if there are no disputes from the cardholder regarding the transaction that was used to collect the "provisional" reference, then the "provisional" status can be changed to permanent status. As the Magensa Registry is populated with transactions from various sources, statistical evidence of authenticity, in the absence of disputes or charge- backs, can be generated without assistance from the card issuer.



Financial

ATM • Card Personalization & Issuance • Teller Window • POS • Remote Deposit Capture • Mobile • Internet Banking • Law Enforcement

Government

Alcohol, Tobacco & Firearms • Dept of Motor Vehicles • Election • Legislative Regulations • Social Security • Remote Access • Law Enforcement

Retail

POS • Store Controller • Merchant Host • Processor Gateway • Acquirer • Brand Switch • Issuer • Law Enforcement

eCommerce

• Banking and financial institutions • eProcurement • Cloud-based services • Gaming • Marketplace services • mCommerce • Merchants • Pharmacy and Healthcare • Service providers • Social Networks/Dating • Law Enforcement

Enterprise

Content & Delivery • Facilities Access Control • Forms Management • IP Property • New Hire ID • User Identity • Remote Access • Law Enforcement

Global MagnePrint® Exchange

Shared and accessible fraud information database, cross-industry collective data MANAGEMENT & AUTHENTICATION OF: Cards, Keys, Users, Hosts, Tokens, Devices.

Exceeds FFIEC recommendations and PCI DSS compliance.

Conclusion

The MagnePrint system has been exposed to rigorous test environments of statistically significant size, with quantifiable positive results. Following are some of the most prominent benefits associated with the adoption of the MagnePrint risk management tool.

Decline in direct skimming: As it is continually adopted, MagnePrint will have greater impact on the success of skimming - a method for creating counterfeit cards in which a legitimate string of card data bytes is captured and copied to create another card. Counterfeit cards created by skimming are easily detected by MagnePrint technology. The decline in skimming will lead to a decline in credit, debit and ATM card fraud losses.

Diminished Harm from Data Breaches: Counterfeit cards created by breach of a cardholder database are easily detected by MagnePrint technology. The lack of profit from a data breach will de-incentivize the criminals. Fewer data breaches will lead to a decline in credit, debit, and ATM card fraud losses.

Other benefits: MagnePrint technology will increase the confidence and goodwill among both cardholders and merchants. Although difficult to quantify, this benefit is significant. With the increased awareness in identity fraud, consumers are becoming concerned with fraudulent uses of their credit and debit cards.

Furthermore, both issuers and acquirers will benefit over time in the form of lower acquisition costs, lower churn levels and increased card activity.

Secured By MagneSafe

Magensa can supply all the necessary components of the system, including readers, PIN pads, and card issuing equipment, all certified as MagneSafe. MagneSafe is the technology umbrella used by Magensa that combines strong cryptography, data masking, multi-factor authentication and the MagnePrint risk management tool, enabling it to prevent or detect fraud, and alert or advise its clients of its risk assessment.

MAGENSA™
SIMPLY STOPS FRAUD

Magensa is a fraud prevention, detection and advisory service. It maintains a globally accessible registry of authentication information so that consumers, financial institutions, retailers, businesses and governments can assess the validity and trustworthiness of the credentials and products they rely upon in the course of online identification, payment, and other important transactions. Additionally, Magensa provides token management and cryptographic services, vital to the protection of cardholder data, the payment system, and personal or sensitive information. Magensa is a subsidiary of MagTek, Inc.

Magensa, LLC | www.magensa.net|

Registered to ISO 9001:2008 © Copyright 2015 Magensa, LLC. PN D99875442 REV 20 8/15