Introduction

A recent spate of data breaches at major international retailers has put the spotlight on the threat to cardholder security posed by compromised point-of-sale (POS) systems. But an equally large threat looms in the form of e-commerce firms storing their customers' card data to facilitate recurring or repeat purchases. This white paper outlines the threat posed by such "card-on-file" practices, and how mobile payment technologies can **free e-commerce firms from the burdens and risks of retaining these financial data**, allowing them to focus on their real business of serving customers.

The Problem

The practice of card on file (sometimes abbreviated as "CCOF" from "credit card on file") is most common in the United States, as European banks have traditionally barred merchants from storing credit and debit card data. However, CCOF impacts individuals and retailers in other parts of the world, if only because of the reach of those global firms which keep customer card data. (For example, between them Apple and Amazon are said to have approximately 1 billion cards on file.) And with recurring charges and a speedy checkout being increasingly seen as crucial building blocks for e-commerce success, it is more likely that CCOF and related practices will gain rather than lose acceptance around the world.

Despite ongoing attempts to mitigate the risks associated with CCOF, such vulnerabilities are impossible to eliminate. Because **most CCOF systems contain enough data to initiate and complete transactions**, once a user registers their "visible" card details and personal information, the only thing protecting against unauthorized charges are data encryption and database protection and monitoring. And as has been demonstrated time and time again - most recently with breaches in Apple's cloud service - even the most secure repositories of customer data remain vulnerable.

Solution Overview

As a result, the only way to eliminate the risks and costs of CCOF is to **replace traditional CCOF systems** with one which does not store the customer's card and personal data in one place, using technology such as Cellum's patented **Split Secret** solution (see below).

Replacing CCOF with a solution in which actual cardholder data is never transferred during the transaction not only serves to effectively prevent unauthorized charges. It can also lead to a "**liability shift**" in which transactions are reclassified in a way that makes them **less expensive to the merchant**, and obviate the need for regular PCI DSS audits and related security costs. Finally, with user consent a merchant can benefit from a larger volume of actionable customer information, including real-time location data.

Click here to watch our video about the importance of security

Solution Details

The key requirement in moving beyond traditional CCOF is **tokenization**, in which usable card information is replaced by **non-sensitive "surrogate" data** not subject to unauthorized decryption. Tokenization swaps out the credit or debit card number and expiration date for numeric codes called a "payment token" and "token expiry date" in a way that they cannot be confused with card numbers. (While tokenization can be used to store other types of data, note that much of the data on a card's magnetic/ISO stripe or EMV chip is always prohibited from being stored by merchants.) The mapping between card numbers and expiration dates and the corresponding payment tokens - and the approval of any "de-tokenization" requests - is the responsibility of a token service provider, which may be the card's issuing bank, a payment network/card scheme, or a technology provider such as Cellum.

There are different approaches to tokenizing cardholder data, but regardless of the architecture of the solution **there are certain practices that must be followed** when creating an effective tokenization system. Overall, the challenge is to create and maintain a system in which tokenization can take place **without creating any unnecessary friction** for cardholders or merchants, while giving end-users the additional confidence offered by the ability to individually confirm all recurring transactions.

Adding tokenization in the e-commerce setting - and thus **shifting liability away from the merchant** - can be most easily achieved by requiring the use of an already-existing customer-facing digital payment system with a proven tokenization element, such as the mobile wallets Cellum has developed for a number of leading banks and telcos in Europe and Asia.

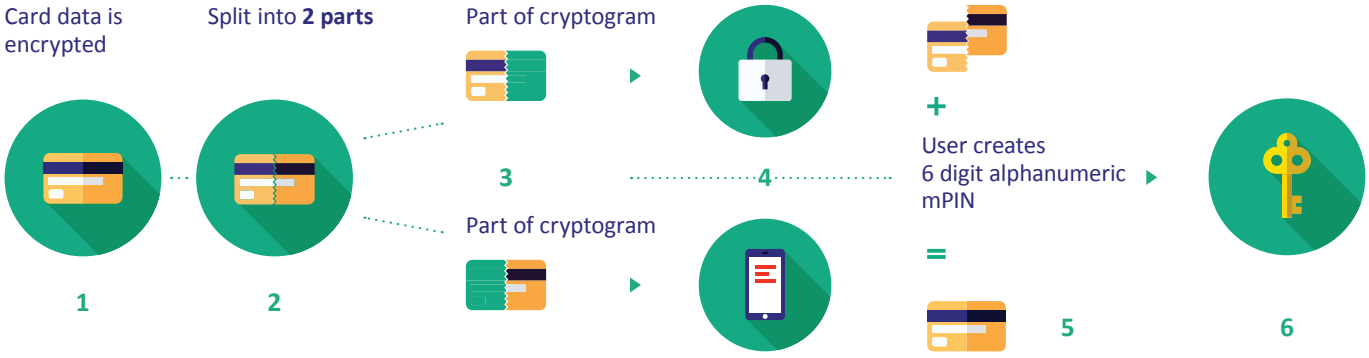
But another approach followed by Cellum and some other leading developers of mobile security systems is to focus on **"platform neutral" tokenization solutions** capable of supporting numerous different types of payment applications. Tokenization can also take place in a manner that effectively hides the process from the customer, freeing them from having to register with a payment app, while at the same time offering the merchant relief from security-related risks.

Cellum's Secret for 100% Security

Cellum's years of research into payment security has resulted in a proprietary, **patented card vault solution** called **Split Secret**. Trusted by major international brands and subject to constant innovation, Split Secret to date maintains a **track record of zero fraud**.

Total security is maintained by the combination of knowledge and possession-based safeguards: In order to make a transaction with a card or payment instrument stored in the vault, the user must know the mPIN and be in possession of the device to which the payment instrument was registered. An advanced card registration process involving a nominal payment in conjunction with a one-time password also ensures that only the legitimate cardholder can add a card to the card vault.

Meanwhile, Split Secret solves the problem of vulnerable card databases by obscuring all card data with AES and RSA encryption and **scattering the resulting fragments across multiple physical locations**. And with the user's mPIN reduced to a keyword for decrypting the cryptogram, the only vulnerability is the (very unlikely) chance that an unauthorized party can guess the password.



Conclusion

As the liabilities posed by traditional CCOF practices become ever more apparent and onerous, tokenization using mobile wallet technologies presents a unique solution to the problem, providing **better security and lower costs** for e-commerce merchants and their customers alike.

Contact

If you are interested in our solutions, you can find out more at www.cellum.com or contact us at sales@cellum.com.