The Agitator

Agitator Guide

to

Dealing with a Reluctant CRM and/or Payment Processor

More—Far More--Than You Should Have to Know

It's a shame you even have to tease your brain with this. But, let's face it some CRMs or Payment Processors will try to hold on to your business by making it extraordinarily difficult to leave.

Of course, a most powerful magnet for keeping you in their clutches is the fear of losing your data on those monthly donors whom you've you spent countless years on investment building.

So, what do you do when you want to change platforms or processors?

First, you want to bring all your sustainers/recurring donors and their data—credit card numbers, home addresses, giving history, email and postal addresses over to the new platform.

Those vendors reluctant to lose your business or angry over your leaving will stall, obfuscate and throw up as many barriers as possible. As in hocus-pocus explanations like: "due to compliance issues, we can't release the credit card data or tokens" …" this is a very laborious, time-consuming, technical process" …" we've never done it before" …" it'll take a lot of time and cost a lot of money." You'd think the process is the equivalent of a NASA space shot.

Nonsense!

The process is truly simple and if they claim it's difficult, they should not be in either the CRM or Payment Processing business.

Unless you have an agreement to the contrary with your vendors, YOUR ORGANZATION OWNS YOUR DATA.

Donor Data, Credit Card Data and PCI Compliance

The two issues they'll quickly raise to as though it's a garlic necklace designed to repel a vampire are the somewhat confusing or complex issues of credit card "tokens" and the issue of "PCI compliance."

Here's the deal.

Basic CRM Data. What we would consider basic donor data—email addresses, postal addresses, gift transactions, notes, etc. are a fundamental part of the CRM. These data can be quickly –as in "with the click of a query button"—be exported from the old to new CRM or directly back to your organization.

Shouldn't take more than a day or two. And sure shouldn't involve much of a charge unless they're intent on ripping you off.

Credit Card Data and PCI Compliance

As a general rule your organization has **no right** to receive the credit card data of a donor. Rather, it must be transferred from one PCI Compliant payment processor to the new PCI Compliant payment processor.

"PCI Compliant" is shorthand for Payment Card Industry Data Security Standard (**PCI DSS**) that is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

So, the only reason the credit card data of your donors can't be –and should not be-- transferred is if you're asking the vendor to move the data to a non-PCI compliant vendor.

Tokens

At the heart of the donor credit card data process is a "token" –an encrypted piece of data that resides on your CRM –and is then used by the Payment Processor to unlock the credit card data and process the gift. Neither the CRM nor you can "see" the credit card information in this token.

So, when it comes to making the transfer the only requirement you need to know is that your credit card data must be transferred to a PCI compliant payment processor.

More on Tokens

In case you're involved in blizzard of excuses you're likely hear the term "token" or "tokenization" tossed around in a manner befitting mission impossible.

So, if you want to argue back and explain it to your vendor or their payment processor here's a quick guide to how tokenization process works.

- CRM captures a credit card number/primary account number (PAN) directly from the donor using a secure form or some type of widget
- The PAN and personally identifiable information (PII) are sent securely to the processor
- The processor encrypts the PAN+PII and returns a token to the CRM
- The CRM stores the token in the database to be used for subsequent charges, like monthly giving

A few comments about the tokenization process:

- The CRM never actually "sees" the PAN, but has access to the PII because the capture process is hosted by the processor
- The token is worthless because it contains zero sensitive information
- The token is essentially a reference to the PAN/PII stored with the payment processor
- The PAN/PII cannot be retrieved using the token, it's for only charging the credit card

Here's how the token transfer process works:

- On the payment processor side, the following information is stored, we'll call this the tokenized data:
- PAN
- Full account number
- Expiration date
- CVV
- Depending on their fraud protection level:

- Last name as it appears on card or full name as it appears on card; and
- Postal code or Full address; and
- CVV code
- Token

Only agreement needed to transfer your credit card information

- The existing processor and new processor need to agree on the following two items:
- An encryption key or certificate to use for the transfer
- Transfer mechanism, either SSH/SFTP or some other secure transfer protocol or service, like Dropbox
- The existing processor then needs to export the tokenized data and encrypt it using the key or certificate from the new processor
- The existing processor then needs to transfer the encrypted tokenized data
- The new processor then needs to download and decrypt the tokenized data
- The new processor needs to load the tokenized data into their system
- The organization then needs to run a single test transaction to ensure the data is validated
- The new processor and the organization need to contact the existing processor and notify them to destroy all related PAN/PII

A few comments on the token transfer process:

- PGP is still regarded as one of the best encryption tools because it’s free
- All transfer mechanisms are just another layer of security because the file is already encrypted

- Loading the tokens into the new provider's system may require a cross-reference because the data types may not match:

- The existing processor may store the token as a "UUID", like "aa0ec71a-cbc3-4f3e-afb6-274276cf38ad"

- The new processor may store a custom token (like Stripe), "card_54kl4m53n1jh122o"

- This means that the new process will need to generate a cross reference between "aa0ec71a-cbc3-4f3e-afb6-274276cf38ad" and "card_54kl4m53n1jh122o", but this should be transparent to the CRM and the organization

##########

Hopefully, we've shed more light than shade on this process. If you have any questions send 'em on to Roger@theagitator.net