

It's Official: Pre-Authorization Data Is In Your PCI Scope

Written by Walter Conway

August 6th, 2012



A 403 Labs QSA, PCI Columnist Walt Conway has worked in payments and technology for more than 30 years, 10 of them with Visa.

Like many QSAs, I frequently get asked whether pre-authorization cardholder data—that is, card data written on paper or stored electronically before the transaction is authorized—is in scope for PCI. My answer has always been that if you have any cardholder data, you must handle it in a PCI-compliant manner. That advice applies whether the data is pre-, post- or somewhere in the middle of the authorization process.

Unfortunately, some vague wording and a quote from the very first PCI Community Meeting caused some merchants to question my conclusion. They argued that cardholder data only comes into PCI scope after the transaction is authorized. We now can put this question to rest. The PCI Council has come out with an official statement to QSAs that all cardholder data is in scope, whenever and wherever it is.

The issue of pre-authorization data came up at the first PCI Community Meeting in Toronto in 2007, where a representative of one of the card brands stated that it felt pre-authorization data was not in scope for PCI. The statement, and subsequent misinterpretation of it, led to questions and a ton of electronic ink in the PCI blogosphere at the time. It also launched the urban myth that merchants do not need to protect pre-authorization data.

Some merchants took this position even further, arguing that they could retain sensitive authentication data, such as card security codes, presumably because those codes would be "pre-authorization" data for future transactions. The myth was reinforced by the wording in Requirement 3.2: "Do not store sensitive authentication data *after* authorization" (emphasis added).

Even though the rest of Requirement 3 (which addresses protecting stored cardholder data) does not have any "before" or "after" references, some merchants, security experts and even QSAs held that pre-authorization data was not in scope for PCI. They held to this position even though Council representatives stated regularly that PCI applied any time cardholder data is stored, processed or transmitted and that pre-authorization data is included.

In the July 2012 issue of the PCI Council's Assessor Update, which is sent to all QSAs, the Council has finally resolved the issue. The "FAQ of the Month" addressed the issue head-on, with a formal statement that pre-authorization data is in scope. The Council's statement says:

PCI DSS applies wherever cardholder data (CHD) and/or sensitive authentication data (SAD) is stored, processed or transmitted, irrespective of whether it is pre-authorization or post-authorization. There are no specific rules in PCI DSS regarding how long CHD or SAD can be stored prior to authorization, but such data must be protected according to PCI DSS while being stored, processed or transmitted.

That seems to settle this issue pretty clearly. As for sensitive authentication data, such as the contents of the magnetic stripe and the security code, the Council added this:

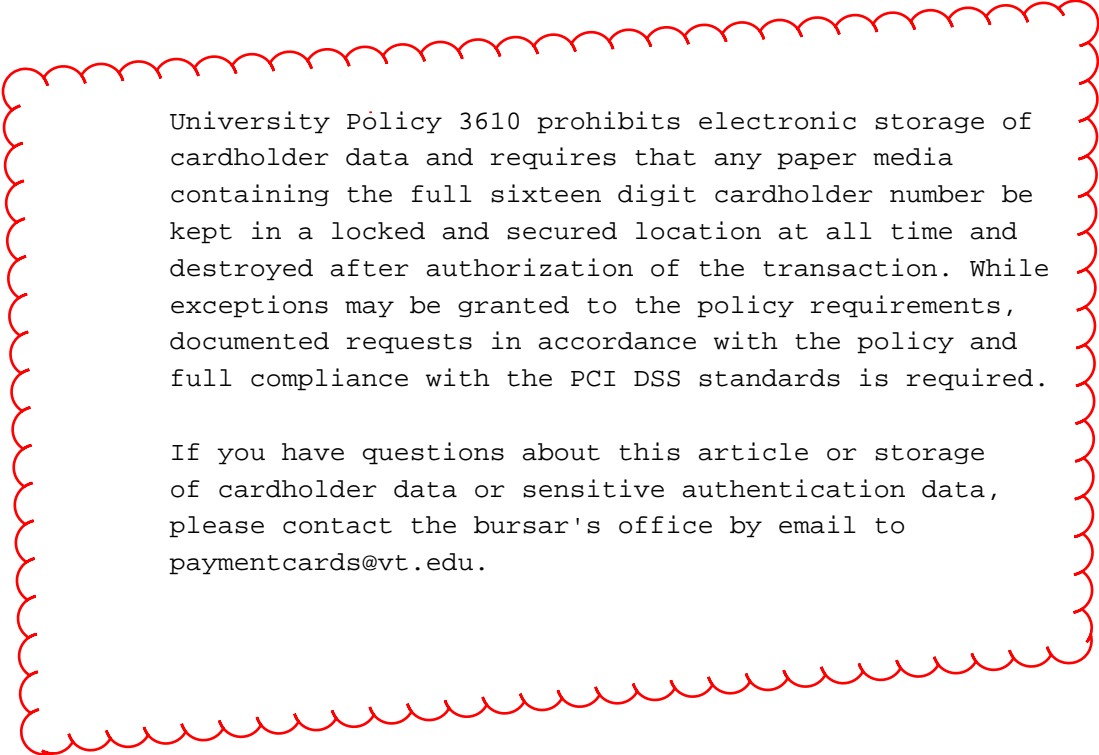
With respect to SAD, PCI DSS Requirement 3.2 prohibits storage of SAD AFTER authorization, even if encrypted. Whether SAD is permitted to be stored prior to authorization is determined by the individual payment brands, including any related

usage and protection requirements. Any permitted storage of SAD prior to authorization would be subject to strict conditions and controls above those defined in the PCI DSS. Additionally, several payment brands have very specific rules that prohibit any storage of SAD and do not make any exceptions. To determine payment brand requirements, please contact the individual payment brands directly.

The bottom line is that cardholder data is in your PCI scope from the time you get it to the time you purge it from your systems (or file cabinets). This conclusion applies to POS devices that are in offline mode, faxes, MOTO or call-center order forms, electronic scans and yellow sticky notes with handwritten PANs.

I'd like to hear what do you think. Either leave a comment or E-mail me.

<https://ssl/>
<http://www/>
<http://storefrontbacktalk.com/text/javascript>



University Policy 3610 prohibits electronic storage of cardholder data and requires that any paper media containing the full sixteen digit cardholder number be kept in a locked and secured location at all time and destroyed after authorization of the transaction. While exceptions may be granted to the policy requirements, documented requests in accordance with the policy and full compliance with the PCI DSS standards is required.

If you have questions about this article or storage of cardholder data or sensitive authentication data, please contact the bursar's office by email to paymentcards@vt.edu.