Location of Cardholder Data and Sensitive Authentication Data

Sensitive authentication data consists of magnetic stripe (or track) data\(^3\), card validation code or value\(^4\), and PIN data\(^5\). Storage of sensitive authentication data is prohibited! This data is very valuable to malicious individuals as it allows them to generate fake payment cards and create fraudulent transactions. See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for the full definition of “sensitive authentication data.” The pictures of the back and front of a credit card below show the location of cardholder data and sensitive authentication data.

Note: The chip contains track equivalent data as well as other sensitive data, including the Integrated Circuit (IC) Chip Card Verification Value (also referred to Chip CVC, iCVV, CAV3 or iCSC).

---

\(^3\) Data encoded in the magnetic stripe used for authorization during a card-present transaction. This data may also be found on a chip, or elsewhere on the card. Entities may not retain full magnetic stripe data after transaction authorization. The only elements of track data that may be retained are the primary account number, cardholder name, expiration date, and service code.

\(^4\) The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

\(^5\) Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Track 1 vs. Track 2 Data

If full track (either Track 1 or Track 2, from the magnetic stripe, magnetic-stripe image in a chip, or elsewhere) data is stored, malicious individuals who obtain that data can reproduce and sell payment cards around the world. Full track data storage also violates the payment brands’ operating regulations and can lead to fines and penalties. The below illustration provides information about Track 1 and Track 2 data, describing the differences and showing the layout of the data as stored in the magnetic stripe.

<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contains all fields of both track 1 and track 2</strong></td>
<td><strong>Shorter processing time for older dial-up transmissions</strong></td>
</tr>
<tr>
<td><strong>Length up to 79 characters</strong></td>
<td><strong>Length up to 40 characters</strong></td>
</tr>
</tbody>
</table>

**Note:** Discretionary Data fields are defined by the card issuer and/or payment card brand. Issuer-defined fields containing data that are not considered by the issuer/payment brand to be sensitive authentication data may be included within the discretionary data portion of the track, and it may be permissible to store this particular data under specific circumstances and conditions, as defined by the issuer and/or payment card brand.

However, any data considered to be sensitive authentication data, whether it is contained in a discretionary data field or elsewhere, may not be stored after authorization.