Blackthorn Compliance

FAQs

Salesforce is PCI DSS Compliant - why do I need Blackthorn Compliance?
Salesforce is indeed PCI DSS Compliant - but what about *your* Salesforce instance?

If you use Email-to-Case, Web-to-Case, API to Case, Customer Communities, or store any external communication at all, you run the risk of customers sending you their credit card numbers. When this happens - your instance is **no longer PCI compliant**.

Are you storing these credit card numbers somewhere?
No! Blackthorn Compliance is a 100% Native Salesforce application - there are **no** 3rd party APIs or packages which in any way store sensitive information.

Do you collect any personal information in the app?
We do not collect any information - zero data is sent outside of your Salesforce instance. We have the email address of the user who installs the application, but this is outside of both the app and your Salesforce instance.

What do you do with any data processed by the app?
Nothing! Blackthorn Compliance does not send or receive data of any kind from your Salesforce instance. Our whole business model is to allow customers to remove sensitive PII data themselves, not to take it and store it somewhere.

You've installed Blackthorn Compliance - great! Now what?
Blackthorn Compliance is already blocking credit card numbers from entering your Salesforce org!

When Blackthorn Compliance is installed in your Salesforce environment, no new records can enter Salesforce with a credit card number. Getting rid of the credit card numbers already in your Salesforce requires an **Audit**. Check out the Blackthorn Compliance User Guide for more information on how to run an Audit.

How does Blackthorn Compliance Work?
Blackthorn Compliance uses a proprietary combination of Regular Expressions **and** the Luhn algorithm. A credit card number must pass **both** criteria in order to be masked:

1. Matches an existing Detection Pattern (Blackthorn Compliance comes with 14 different types)
2. Passes the Luhn algorithm

But what if I have a non-credit card number PII I want to detect (e.g. social security numbers) ?
Great! Blackthorn Compliance comes with several settings which will effectively "skip" the Luhn algorithm.

What does "Detection" mean?
Detection means: "*Block or flag credit card numbers from entering Salesforce*"

For example, when a new Case record is created, and the Description contains a credit card number, Detection will detect the number and **mask** it before the Case is even saved.

What does "Audit" mean?
Audit means: "*Find the credit card numbers already stored in Salesforce.*"

Let's say you have a bunch of Cases from 2016 with credit card numbers stored on them. You would simply configure an Audit to run across all Cases in 2016. The audit will automatically find the credit card numbers, mask them, and send you an email when it's done.

But what if I don't want to mask the numbers?
Great! You can also simply "*Report*" the records which are flagged as containing credit card numbers. Blackthorn Compliance will generate a report with all of the flagged records. Then, you can manually remove the numbers from the records later.

What about bank information, CVVs, social security numbers, and other PII?
Any type of PII is detectable and maskable with Blackthorn Compliance! Check out the Blackthorn Compliance User Guide for how to set up your own *Detection Patterns*.

What objects does Blackthorn Compliance support?
The short answer: all objects!

The longer answer is that while Blackthorn Compliance can be extended to support any object in Salesforce, it is pre-configured to support the following objects:

Object	Preconfigured Detection Fields

Attachment	Body
Case	Subject,Description
CaseComment	CommentBody
ContentVersion	VersionData
EmailMessage	Subject,TextBody
FeedItem	Title,Body
FeedComment	CommentBody
LiveChatTranscript	Body
Task	Subject,Description
SocialPost	Content
SocialPersona	Bio

But what if I have other fields that might contain credit card numbers?
Simply add any text (text, text area, or long text area) field to the Blackthorn Compliance settings and it will be included in both Detection and Auditing!

Sometimes customers take *screenshots* of their credit card numbers and send us an *attachment* - can Blackthorn Compliance detect these?
Yes! We have built an add-on product called **SecureAttachment**. This extends Blackthorn Compliance to detect any type of PII in Attachments and Files (Salesforce Content). Please send us an email for more information!

I tried using my credit card and Blackthorn Compliance didn't work - what gives?
Blackthorn Compliance comes with **15** credit card "Detection Patterns" - these are anything but an exhaustive list of credit card types out there. If you have more types you would like to add, you can create your own Detection Patterns. This requires **zero code**.

1. These are the "Detection Patterns" Blackthorn Compliance comes with:
    a. Amex
    b. Discover
    c. JCB
    d. MasterCard
    e. Visa
    f. China UnionPay
    g. Diners Club Carte Blanche
    h. Diners Club

i. Interpayment
j. Instapayment
k. Maestro
l. Dankort
m. Solo
n. UATP
o. US Social Security Number

2. Blackthorn Compliance will detect the following formats:
    a. 4111111111111111
    b. 4111 1111 1111 1111
    c. 4111-1111-1111-1111
    d. 4111*1111*1111*1111
    e. 312456789041111111111111109876543
    f. “Here is my valid credit card 4111111111111111 thanks!”

3. Blackthorn Compliance will not detect these formats:
    a. 4111%1111&1111*1111