Blackthorn Compliance User Guide

Contents

Overview

If your business fails to become PCI compliant, you could be putting your business at greater risk from the growing threat of payment card data breaches and theft, which may result in substantial penalties (such as fines from banks, regulatory agencies, and card associations), fraud and chargebacks, as well as legal costs and lost customers. If your business experiences a data security breach, you could even lose your ability to process credit card payments. Perhaps more importantly, you risk the loss of customers.

If you use Salesforce for Email-to-Case, Web-to-Case, API to Case, Customer Communities, or store any external communication at all, you allow the risk of customers sending you their credit card numbers. When this happens - you are **no longer PCI compliant**. Despite training customer service agents to delete credit card numbers they find, many credit cards will be unintentionally stored in Salesforce. The last thing a company wants is for customers to find out that they've been storing their unencrypted credit cards numbers.

Blackthorn Compliance **automatically** detects and masks credit card numbers *before* they enter Salesforce, and audits your org to mask credit cards *you already have*. The 100% native app helps to keep companies PCI compliant - and to avoid hefty penalties & brand tarnishing impact of a credit card data breach.

Installing Blackthorn Compliance

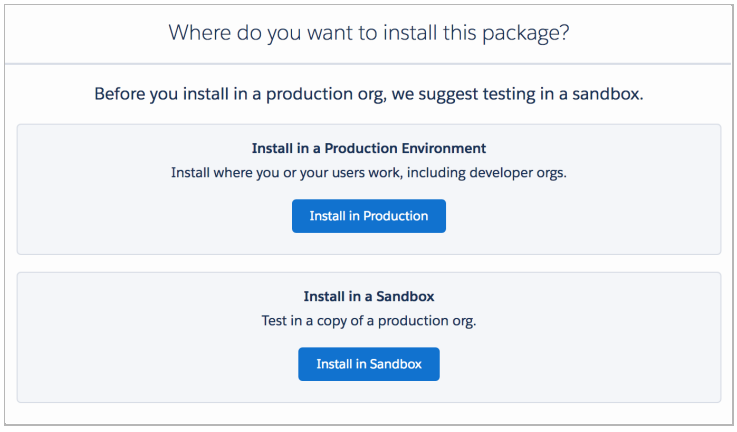
Follow the steps below to install the Blackthorn Compliance package:

1. Navigate to the AppExchange from your Salesforce org or go directly to the AppExchange listing for Blackthorn Compliance at the following URL: https://appexchange.salesforce.com/appxListingDetail?listingId=a0N3A00000EcvUUUAZ

2. Click the 'Get It Now' Button from the AppExchange listing

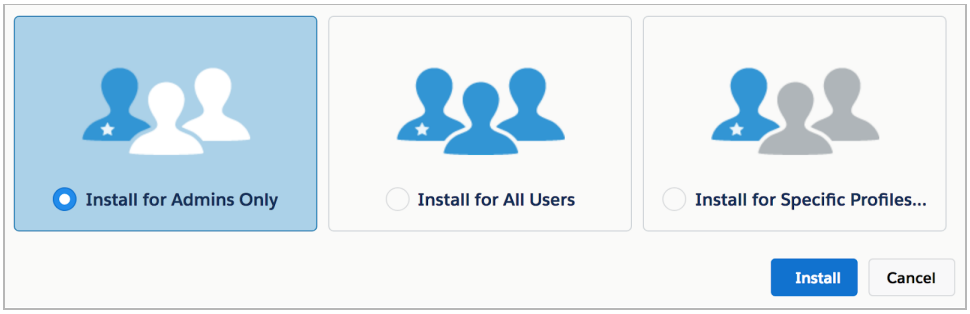
3. Select log into the AppExchange with your Production Salesforce credentials

4. Select the environment where you'd like to install Blackthorn Compliance



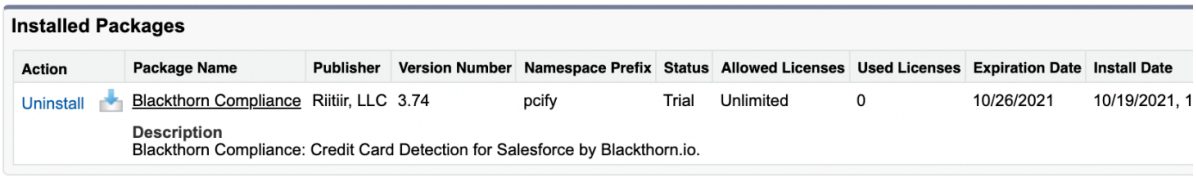
5. If you are already logged into the Salesforce instance where you will be installing, you'll be redirected to a confirmation page for the installation. Otherwise, if you are installing to a different instance of Salesforce, you will be brought to a login screen where you can enter the credentials for that environment.

6. Next, you'll be prompted to select the profiles that will be able to access the installed application. Leave the default of '**Install for Admins Only**' selected and then click the Install button



7. Blackthorn Compliance is now going to install in your Salesforce org
    a. In most cases, this page will automatically refresh noting that the package was either successfully installed or it failed installation.
    b. For orgs that have complex logic/code already applied, it may take longer for the installation process. In this case, an email will be sent to the email address associated to the user who performed the installation either confirming success or failure of the installation
    c. Check out "**Installation Troubleshooting**" for common installation issues

8. After installation, on the list of Salesforce Installed Packages in the Setup, you can see the Blackthorn Compliance package:



9. When the installation for Blackthorn Compliance is completed, you are ready to **Configure Blackthorn Compliance**.

How Blackthorn Compliance Works

You've installed Blackthorn Compliance -- now what? Good news! 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.

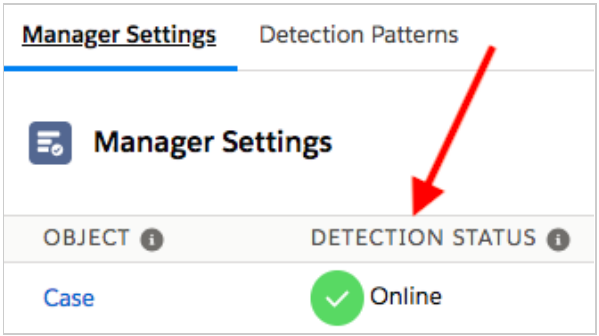
Our credit card detection technology uses a combination of *Regular Expressions* and the *Luhn Algorithm*. A credit card number must pass **both** criteria in order to be masked:

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

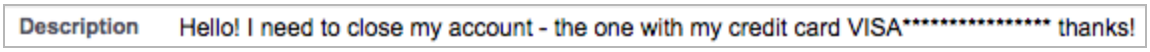
We've created a feature called **Detection** which combines these approaches.

Detection

Detection is Blackthorn Compliance-speak for "*stopping credit card numbers from coming in*". Blackthorn Compliance Detection processes entire strings of text for numbers which match the format of known credit card issuers. Not only that, but Blackthorn Compliance also determines whether the detected number is a **valid** credit card. This is important because there are lots of other numbers which match similar credit card number formats: order numbers, phone numbers, etc. Blackthorn Compliance never masks a number unless it is a completely valid credit card number.



For example, when a new Case record is created, and the Description contains a number which matches a known issuer format, Blackthorn Compliance will check whether the number is a valid credit card. If the number is a valid credit card, then Blackthorn Compliance will appropriately mask the number **before** the Case is even saved.



What Types of Credit Cards Does Blackthorn Compliance Detect?

While we're pretty good at detecting credit cards, we can't predict the format of *every* type of credit card on the planet. Blackthorn Compliance comes with matching patterns for the following credit card issuers:

1. American Express
2. Discover
3. JCB
4. MasterCard
5. Visa
6. China UnionPay
7. Diners Club Carte Blanche
8. Diners Club
9. Interpayment
10. Instapayment
11. Maestro
12. Dankort
13. Solo
14. UATP

Note: If you need to detect credit card number types not listed here or other PII (e.g. social security numbers) then check out "**Detection Patterns**".

But what if the credit card isn't in the right format?

It doesn't matter! Blackthorn Compliance will detect the following formats:

- 4111111111111111

- 4111 1111 1111 1111
- 4111-1111-1111-1111
- 4111*1111*1111*1111
- 312456789041111111111111109876543
- “Here is my valid credit card 4111111111111111 thanks!”

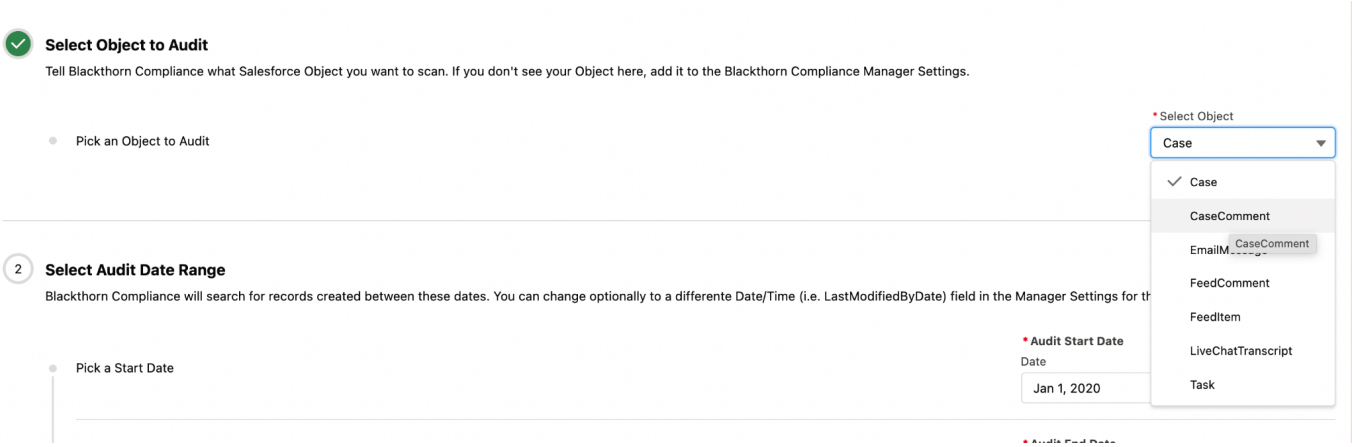
Here are some examples of what Blackthorn Compliance will **not** detect:

- 4111%1111&1111*1111

Tip: Always keep Detection ON.

Audit

Auditing is Blackthorn Compliance-speak for “*finding the credit card numbers already stored in Salesforce*”. Audit actually uses the exact same technology as Detection, except it scans your historical Salesforce data for credit card numbers.

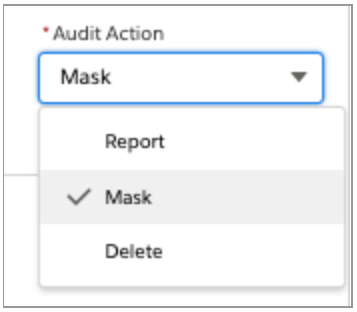


Example: Let’s say you have a bunch of Cases from 2016 with credit card numbers stored on them. You would simply configure an Audit to run across all Cases in 2016. Audit will automatically find the credit card numbers, mask them, and send you an email when it’s done.

When you have completed an Audit, Blackthorn Compliance stores the results in records called “**Logs**”. These Log records drive the native reporting and dashboards for Blackthorn Compliance. Check out the section “**Blackthorn Compliance Analytics**” for more information on Audit results.

Detection and Audit Actions

Actions in Blackthorn Compliance are "*what happens when you find a credit card number*". The default action is to mask the number upon detection, but you are also able to Report and Delete records.



Mask

When a credit card number is detected, the default (and recommended) Action is **Mask**. This means that the credit card number is masked, and *permanently* removed from your Salesforce org. This is NOT the same as *encryption* - you cannot get the data back once it's been masked!

Report

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. You would still need to manually remove the numbers from the records later.

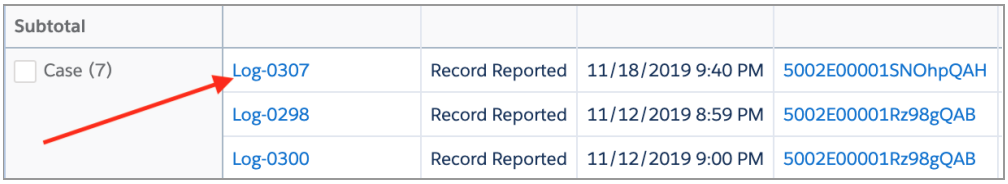
Delete

Better safe than sorry! For some customers, they don't want to risk the chance of storing any PII. If a customer sends their credit card number to you, what's the likelihood that they'll send other sensitive information?

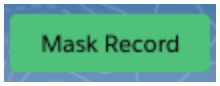
Selecting "Delete" for your Audit or Detection Action will delete the entire record if a credit card number is detected. For example, if a valid credit card number is detected in the body of an Email Message - the entire record is deleted.

How to manually remove credit cards reported by Blackthorn Compliance

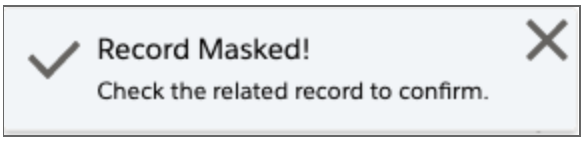
1. Click on the **Reports** tab
2. Open the Folder **Blackthorn Compliance Reports**
3. Select any of the following reports:
    a. Credit Cards Reported All Time
    b. Credit Cards Reported This Month
    c. Credit Cards Reported Today
4. Click on the field in the report **Log: Log Number**



5. Press the **Mask Record** button

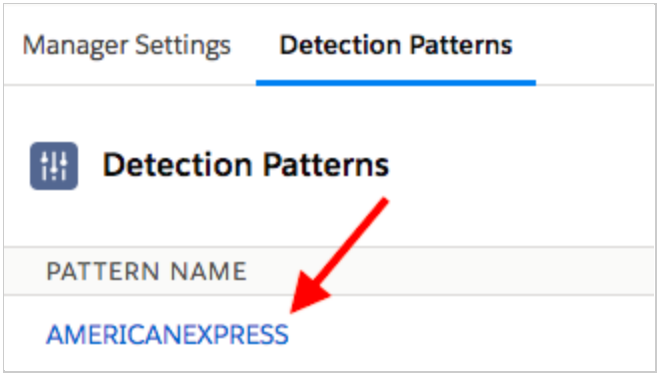


6. You should see a successful mask message:



Detection Patterns

Detection Patterns are how Blackthorn Compliance finds credit card numbers and other PII. We use a combination of Regular Expressions (RegEx) to match specified patterns of numbers. The Custom Metadata Type “DetectionPattern" comes pre-configured with 15 patterns. These patterns are the *most likely* instances of credit card numbers to be found in your Salesforce org. You may turn some of these off if you would like, and you can even add your own patterns!



Credit card numbers are given special treatment in Blackthorn Compliance. When a Detection Pattern is a "**Credit Card Pattern**", we go beyond a simple RegEx match - we also make sure that the credit card number is *valid*. This way we can avoid false positives getting masked accidentally. Check out the section "**Configure Detection Patterns**" for how to set up your own patterns.

What Objects Does Blackthorn Compliance Support?

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
Case	Subject,Description
CaseComment	CommentBody
Task	Subject,Description

Instant upgrades are available for the following objects:

Object	Preconfigured Detection Fields	Required Package
Attachment	Body	Blackthorn Compliance, Blackthorn Compliance-Files
ContentVersion	VersionData	Blackthorn Compliance, Blackthorn Compliance-Files
FeedItem	Title,Body	Blackthorn Compliance, Blackthorn Compliance-Chatter
FeedComment	CommentBody	Blackthorn Compliance, Blackthorn Compliance-Chatter
EmailMessage	Subject,TextBody,HTMLBody	Blackthorn Compliance, Blackthorn Compliance-Email2Case
LiveChatTranscript	Body	Blackthorn Compliance, Blackthorn Compliance-LiveAgent
SocialPost	Content	Blackthorn Compliance, Blackthorn Compliance-Social
SocialPersona	Bio	Blackthorn Compliance, Blackthorn Compliance-Social

If you need to detect credit card numbers on other objects in Salesforce then check out "**Extending Blackthorn Compliance**" for how to add your own objects to Blackthorn Compliance.

Configuring Blackthorn Compliance

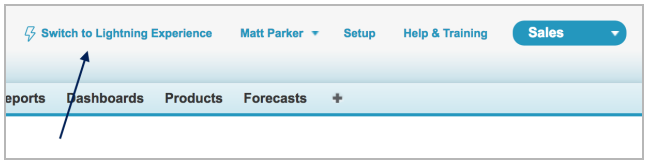
Note: Blackthorn Compliance is a Lightning App. If you are a Salesforce Classic User, you will need to temporarily switch to Lightning Experience before configuring Blackthorn Compliance. You can switch

back to Classic after you're done. It is **not** required to have enabled Lightning Experience for you Salesforce Org or any Users.

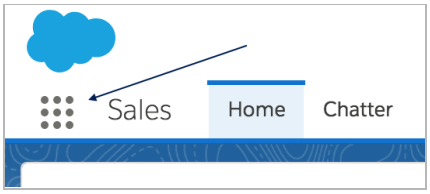
When you install Blackthorn Compliance - nearly all of the configuration is already done for you. Depending on your Salesforce org, you may choose to not make any changes to the default configuration. We recommend that you consider keeping the configuration as-is before making changes.

Setup Configuration

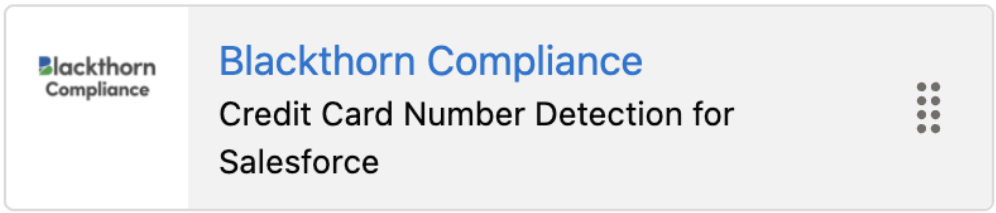
1. If you are a Classic User - click on the Switch to Lightning Experience link. Otherwise skip to step 2.



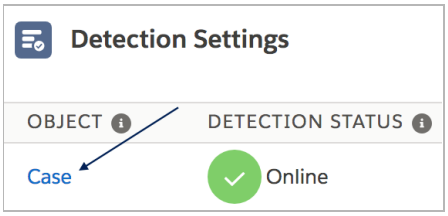
2. Open the App Launcher menu



3. Select **Blackthorn Compliance**

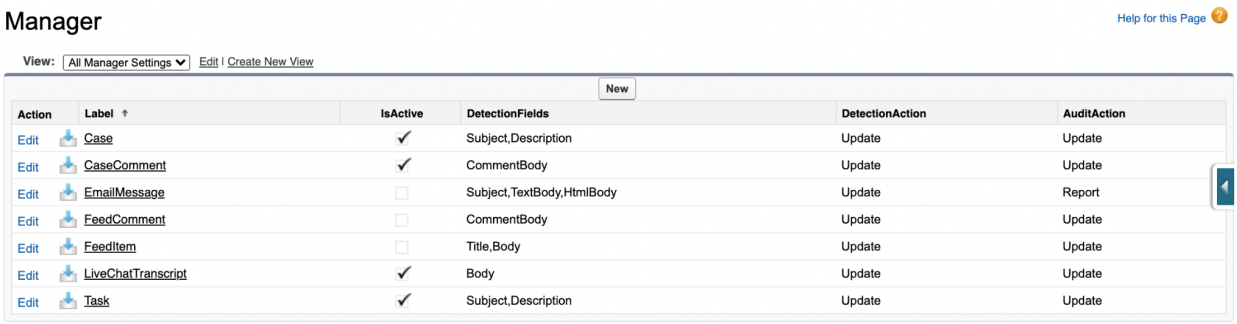


4. If you want to configure a specific object - click on the object name:

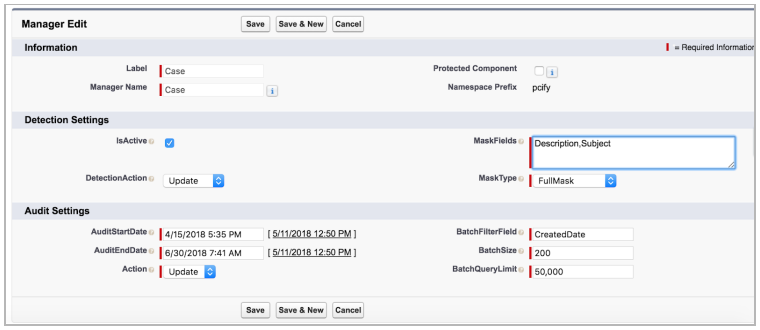


5. Otherwise navigate to: **Setup > Custom Code > Custom Metadata Types > Manager > Manager Records**

6. You should see a list of Manager records



7. Press **Edit** on the object you wish to configure



8. Enter **Detection Fields** for Credit Card Detection
    a. Enter the API names of each **Text** field you think could contain credit card numbers (Text, Text Area, or Text Area Long only) delimited by a comma (,)
    b. Example: “Subject,Description,CustomField__c”

Tip: Blackthorn Compliance comes pre-configured with certain standard fields already added. If you don't store customer communication in other fields, then you do not need to do anything.
Note: Don't add a comma at the end or any spaces!

9. Select **Detection Action**
    a. Update
        i. Update **masks** credit card numbers Blackthorn Compliance detects on records.
        ii. Blackthorn Compliance will create a Log record when this action occurs
    b. Report
        i. Report will create a Log record when this action occurs but will **NOT** mask the credit card number. You can view the reported records in the Blackthorn Compliance Reports Folder.
10. Select **Audit Start Date**
    a. Date from which Audit will start querying for records
11. Select **Audit End Date**
    a. Date at which Audit will stop querying for records
12. Select **Audit Date Field**
    a. Datetime field for Audit to use in its query

Example 1: a Start Audit Date of 5/1/2018 and an End Audit Date of 5/31/2018 and the Batch Filter Field is "CreatedDate" will query for *all records that have been created in May*.
Example 2: a Start Audit Date of 1/1/2012 and an End Audit Date of 12/31/2012 and the Batch Filter Field is "LastModifiedDate" will query for *all records that were last modified in 2012*.

13. Select **Audit Action**
    a. Update
        i. Update **masks** credit card numbers Blackthorn Compliance detects on records.
        ii. Blackthorn Compliance will create a Log record when this action occurs
    b. Delete
        i. Delete will delete the **ENTIRE** record if a credit card number is detected in **ANY** field.
        ii. Blackthorn Compliance will create a Log record when a this action occurs
    c. Report

i. Report will create a Log record when this action occurs but will **NOT** mask the credit card number. You can view the reported records in the Blackthorn Compliance Reports Folder.

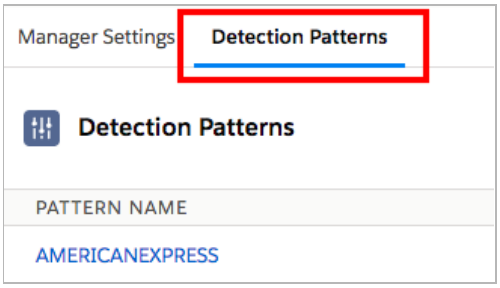
14. Select **Audit Batch Size**
    a. Defaults to 200
    b. 2000 is the maximum Batch Size

15. Select **Audit Query Limit**
    a. Defaults to 50,000
    b. 50 million records is the maximum number of records retrievable by a Database.QueryLocator query: https://developer.salesforce.com/docs/atlas.en-us.apexcode.meta/apexcode/apex_batch_interface.htm
16. Press **Save**
17. Navigate back to the Blackthorn Compliance Lightning App

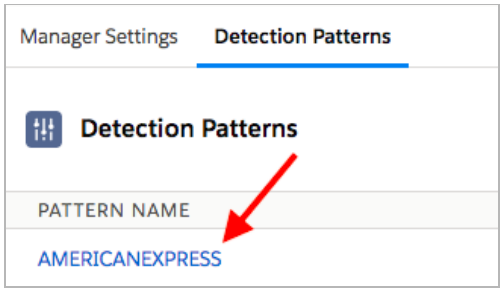
Configure Detection Patterns

Configure Blackthorn Compliance Native Patterns

1. Select the tab “Detection Patterns”



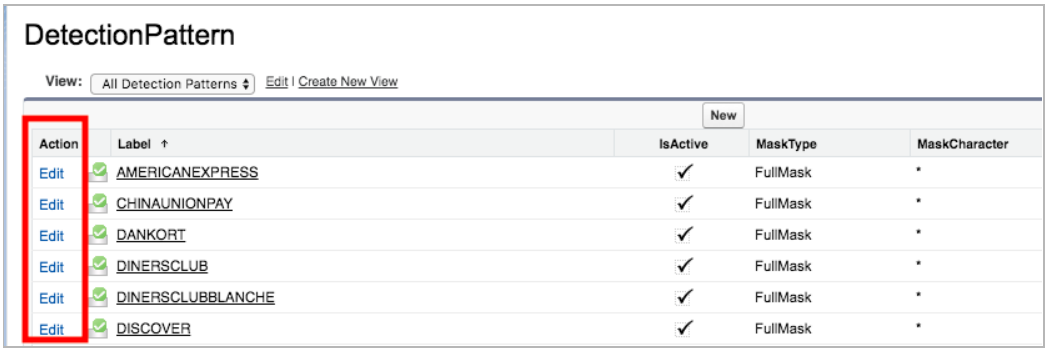
2. Click on the Detection Pattern Name



3. If you're already in the Setup, navigate to: **Setup > Custom Code > Custom Metadata Types > DetectionPattern > Manage DetectionPattern**

4. You should see a list of Detection Patterns

5. Click **Edit** on the Pattern you wish to configure

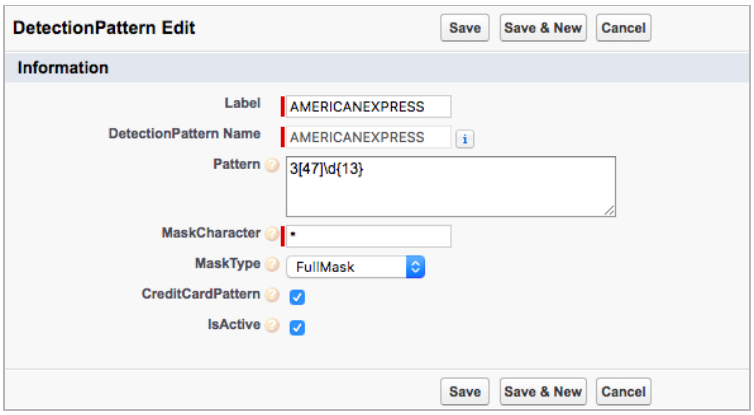


6. Select **Mask Character**
    a. Enter any single character you want to mask PII numbers with - the default is an asterix (e.g. AMERICANEXPRESS**********) but you could use an X, #, @, or any other single character you need.
7. Select **Mask Type**
    a. **Full Mask**: all characters are masked
    b. **Last4**: all credit card number characters are masked but the last 4 characters
        i. AMERICANEXPRESS**********1234
    c. **First6andLast4**: all credit card number characters are masked but the first 6 and the last 4 characters
        i. AMERICANEXPRESS123456******1234

ii. **Tip**: It is recommended that you only store the minimum amount of credit card digits you need to verify customer accounts.

Create your own Detection Patterns

1. Navigate to **Setup > Custom Code > Custom Metadata Types > DetectionPattern > Manage DetectionPattern**
2. Click "**New**"



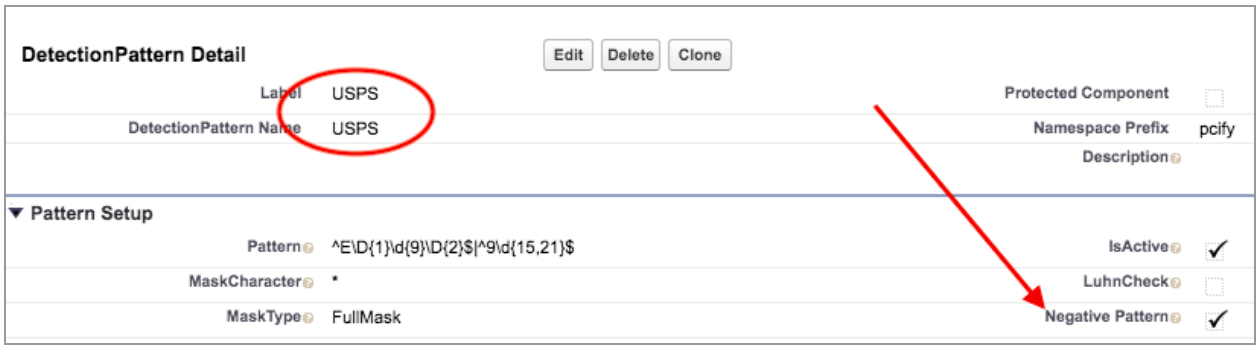
3. Enter a **Label**
    a. Must be unique
4. Enter a **DetectionPattern Name**
    a. Must be unique
5. Enter a **Pattern**.
    a. This pattern must be a valid Java Regular Expression.
6. Enter a **Mask Character**
7. Enter a **Mask Type**
8. If the pattern is for *credit card numbers*, check the box **LuhnCheck**

a. When this box is checked, all numbers matching this pattern will go through a Luhn algorithm check for credit card number validity.
b. If this box is unchecked, all numbers matching this pattern will skip the Luhn algorithm.

9. Check the box **IsActive**
10. Press **Save**

Congrats! You have just created a new Detection Pattern for Blackthorn Compliance. Be sure to check a few dummy records to make sure the RegEx is correct.

Negative Detection Patterns



Have you ever experienced a false positive before? Was it a tracking number that resembled a credit card number? With **Negative Detection Patterns**, you can effectively exclude these numbers from Blackthorn Compliance detection. All you need to do is create your own patterns for international phone numbers, UPS, USPS, Fedex, and other common false positives numbers.

Some things to note:

- Numbers matched with Negative Patterns **are not masked**.
- It is possible for a record to have both valid credit card numbers and false positives.
- It is also possible for the *same number* to be both a valid credit card number and a false positive.

Create Negative Detection Patterns

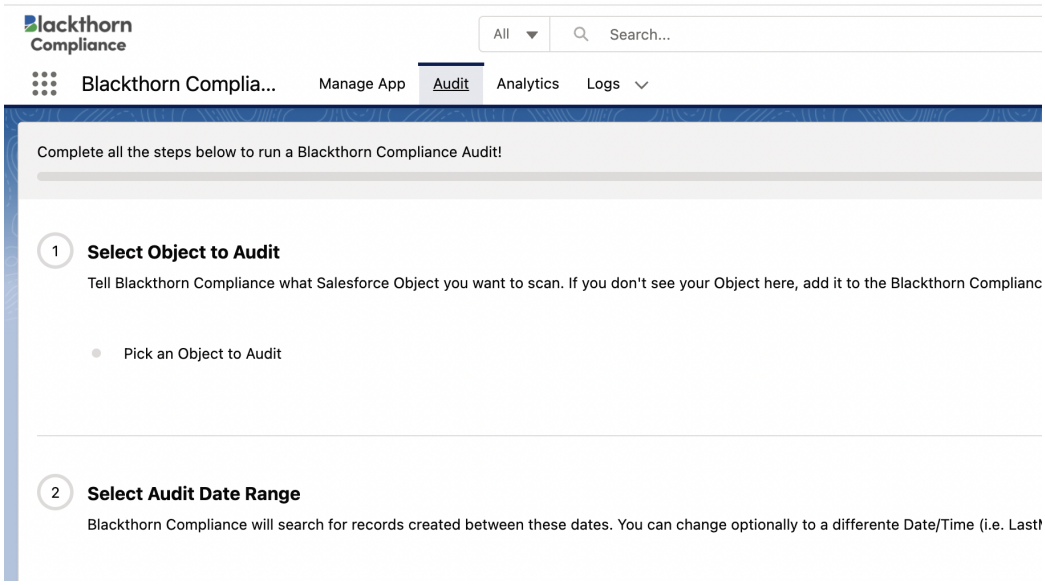
1. Navigate to **Setup** > **Custom Code** > **Custom Metadata Types** > **DetectionPattern** > **Manage DetectionPattern**
2. Click "**New**"
3. Enter a **Label**

    a. Must be unique
4. Enter a **DetectionPattern Name**
    a. Must be unique
5. Enter a **Pattern**.
    a. This pattern must be a valid Java Regular Expression.
6. Check the box **Negative Pattern**
    a. This must be true
7. Check the box **IsActive**
8. Press **Save**

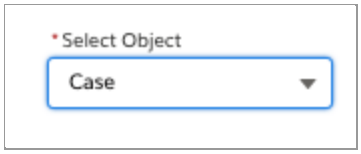
How to Run an Audit

Auditing is an important part of any Blackthorn Compliance implementation. Auditing is how you get rid of all the PII that you already have in your org. Follow the steps below to easily scan any Salesforce records for PII.

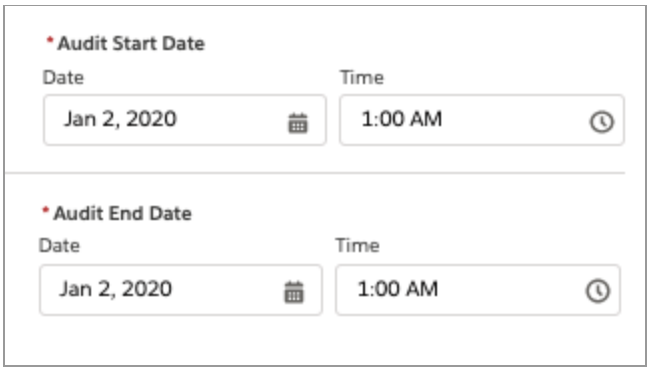
1. Navigate to the **Audit** tab:



2. Select an **Object** to Audit



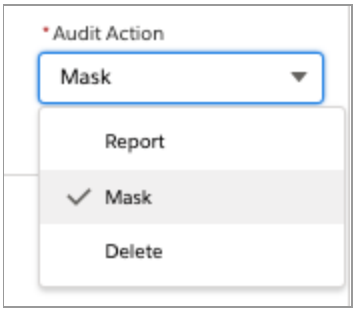
3. Select **Audit Start Date** and **Audit End Date**



Audit Start Date is the *Created Date* from which Audit will start querying for records. Audit End Date is the *Created Date* at which Audit will stop querying for records

Note: You can change the default Audit date range field to any other DateTime field (such as LastModifiedDate) by changing the AuditDateField in the Manager Custom Metadata Type.

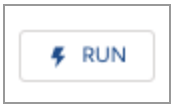
4. Select **Audit Action**



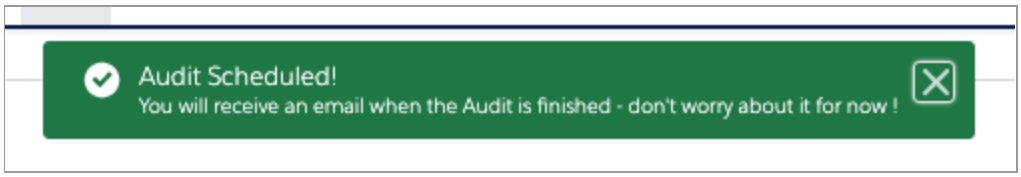
Mask will permanently redact credit card numbers Blackthorn Compliance detects on records according to the Mask Type configured for that record's object. **Report** will create a Blackthorn Compliance log record if a credit card number is detected but will *NOT* mask the number. You can view the reported records in the Blackthorn Compliance Reports Folder. **Delete** will delete the *ENTIRE* record if a credit card number is detected in *ANY* field.

Note: Existing EmailMessages do not support Mask. More information here: https://developer.salesforce.com/docs/atlas.en-us.object_reference.meta/object_reference/sforce_api_objects_emailmessage.htm

5. Press **RUN**



6. You should see the following success alert:



7. You will receive an email confirmation with the job is done.

Note: Depending on the Audit dates selected, and the Audit Action, the Audit could take a few minutes to a few hours. We recommend testing your first audit with a month, and then expanding the date range to include years of records.

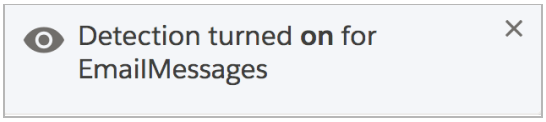
Configure Blackthorn Compliance for Email-to-Case

If you have Email-to-Case enabled for your Salesforce org, and would like Blackthorn Compliance to scan Email Messages you can simply contact us for an instant upgrade: contactus@riitiir.com

Once the upgrade is completed, all you need to do is turn on Detection for Email Message:

1. Turn on Detection

2. You should see the following alert notification



3. Congratulations! You have successfully configured Email Messages for Blackthorn Compliance.

Note: You still need to install Blackthorn Compliance from the AppExchange listing, but we will upgrade your existing package to include Email-to-Case support.

Configure Blackthorn Compliance for Chatter

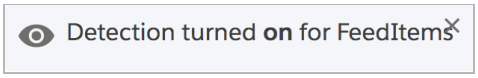
If you have Chatter enabled for your Salesforce org, and would like Blackthorn Compliance to scan Feed Items and Feed Comments you can simply contact us to upgrade:

https://community.blackthorn.io/s/support

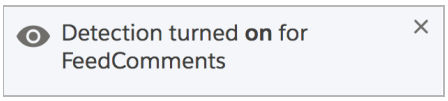
Once the upgrade is completed, all you need to do is turn on Detection for Feed Item and Feed Comment:

1. Turn on Detection for FeedItem

2. You should see the following alert notification



3. Turn on Detection for FeedComment
4. You should see the following alert notification



5. Congratulations! You have successfully configured Email Messages for Blackthorn Compliance.

Note: You still need to install Blackthorn Compliance from the AppExchange listing, but we will upgrade your existing package to include Chatter support.

Configure Blackthorn Compliance for Live Agent

If you have Live Agent enabled for your Salesforce org, and would like Blackthorn Compliance to scan Live Chat Transcripts you can simply contact us for an instant upgrade:

https://community.blackthorn.io/s/support

Once the upgrade is completed, all you need to do is turn on Detection for Live Chat Transcript:

1. Turn on Detection

2. You should see the following alert notification

3. Congratulations! You have successfully configured Live Agent for Blackthorn Compliance.

If you are using Salesforce standard feature Sensitive Data Rules, you can use them in tandem with Blackthorn Compliance. Sensitive Data Rules mask known patterns during Live Chats, in browser. Blackthorn Compliance will mask known patterns after the chat has ended, in the Live Chat Transcript object. Read more about Sensitive Data Rules here: https://help.salesforce.com/articleView?id=live_agent_block_sensitive_data.htm&type=5

Note: You still need to install Blackthorn Compliance from the AppExchange, but we will upgrade your existing package to include Live Agent support.

Install SecureAttachment for Blackthorn Compliance: Scan Attachments and Files

SecureAttachment is our tool for scanning incoming Attachments and Files (Content) for PII. If you would like to scan Files and Attachments for credit card numbers, contact us for details: https://community.blackthorn.io/s/support
*Please note SecureAttachment is a paid add-on

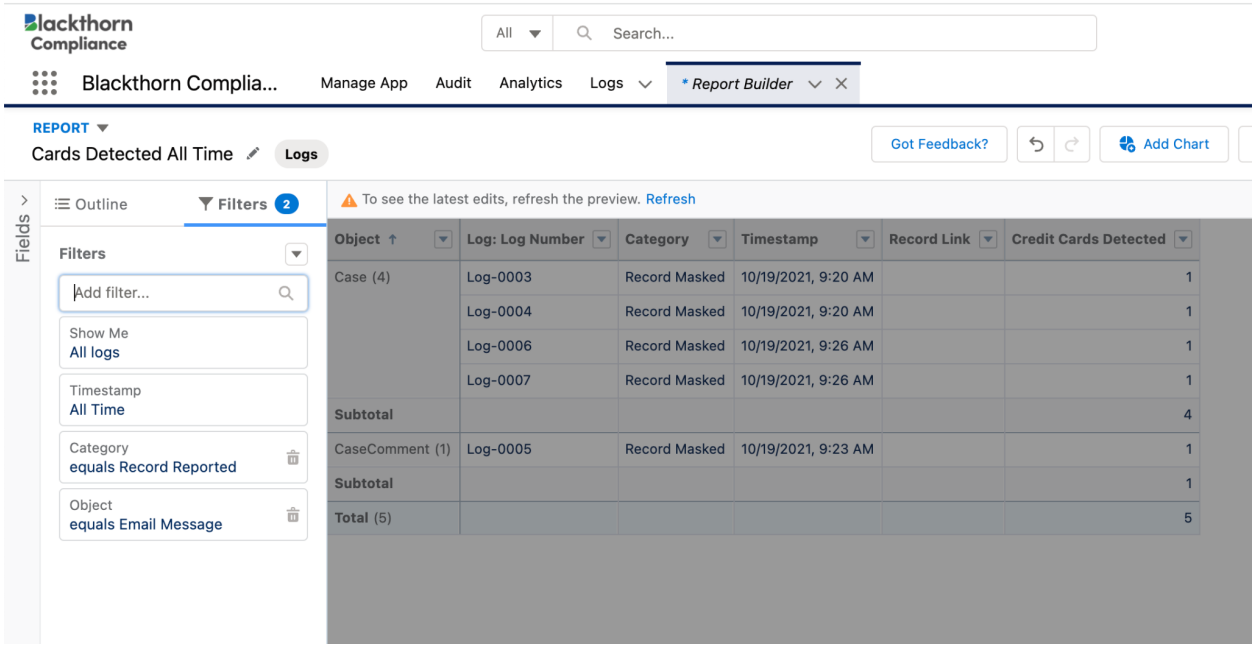
Blackthorn Compliance Analytics

Reporting

Blackthorn Compliance comes with pre-built reports in a Report Folder called **Blackthorn Compliance Reports**. These are completely customizable, and can be combined with your company's internal reporting easily.

The primary source of these reports is the **Blackthorn Compliance Log** object. When a credit card number is detected, Blackthorn Compliance will automatically create a Log with the related record. Any Log field is a potential report filter.

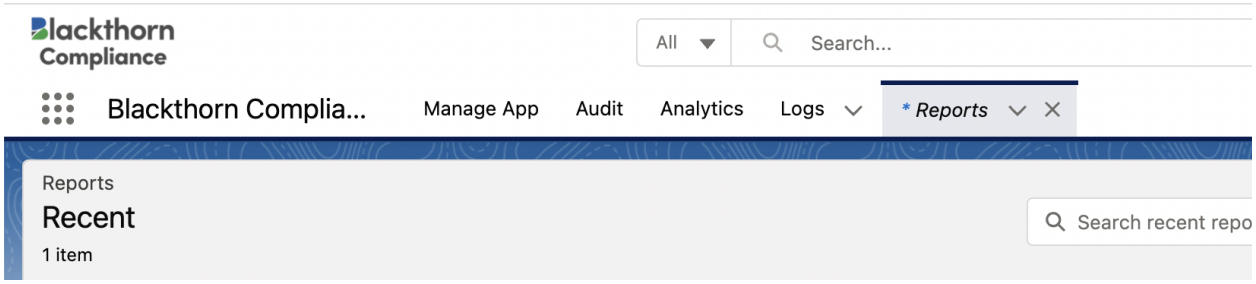
For example, If you only wanted to see Email Messages with credit card numbers detected but **not** masked then you would add the following filters:



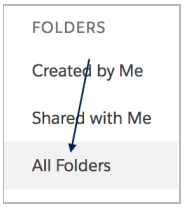
How to find the Blackthorn Compliance Reports

If you want to know where customers are sending you there credit card numbers, and how many numbers they are sending every day, month, or year:

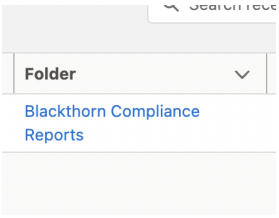
1. Navigate to the **Reports** tab:



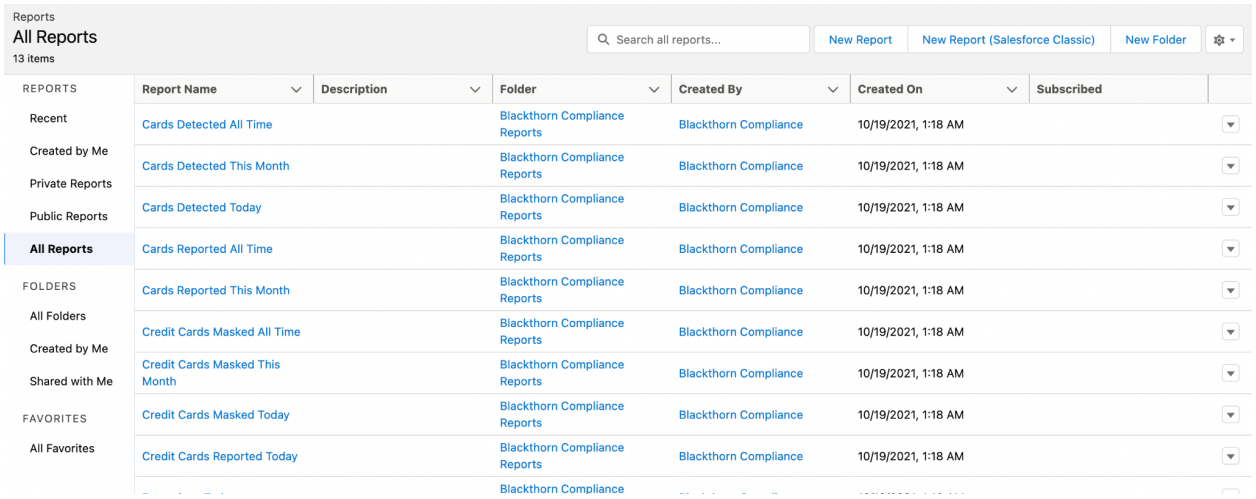
2. Select **All Folders**:



3. Open the Folder **Blackthorn Compliance Reports**

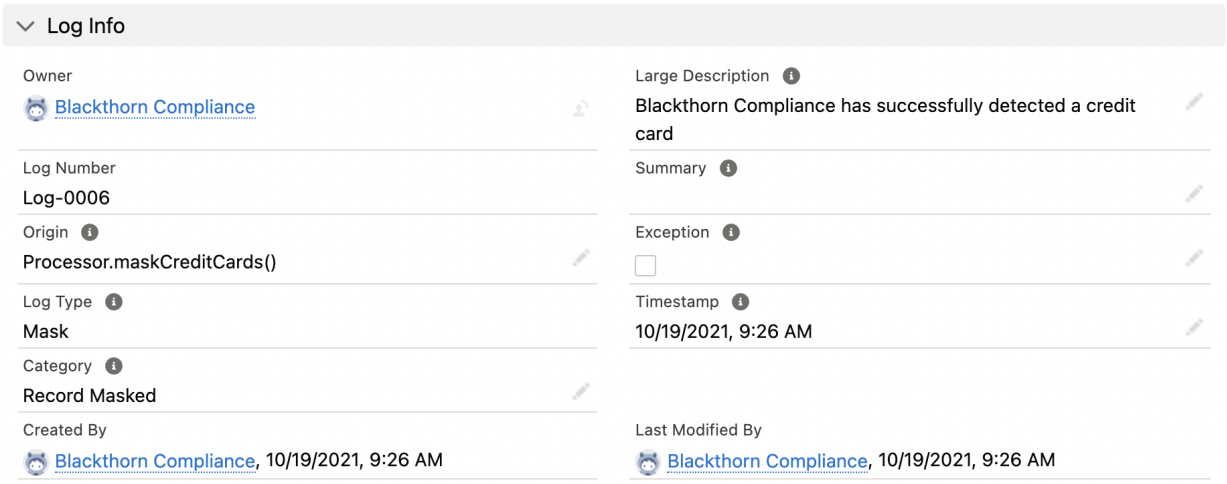


4. Select any of the following reports:



The Blackthorn Compliance Log Object

The Log object is a Blackthorn Compliance managed package object.



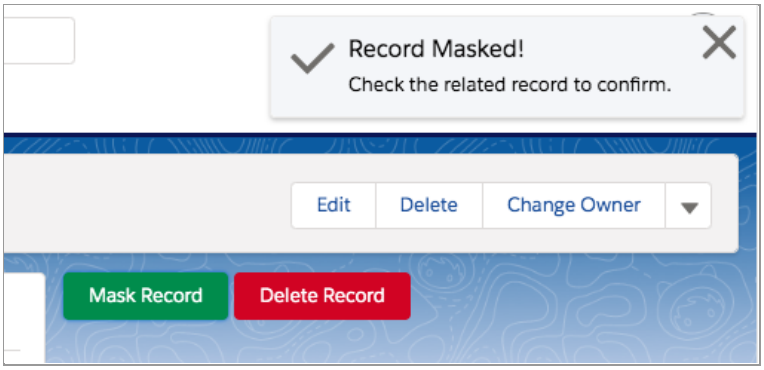
Field Name	Field Type	Field Description	Values
Blackthorn Compliance__RecordId__c	Text	Id of related record	
Blackthorn Compliance__ParentId__c	Text	Id of parent record (for Attachments and ContentVersion records)	
Blackthorn Compliance__RecordLink__c	Formula	Hyperlink to related record	
Blackthorn Compliance__ParentLink__c	Formula	Hyperlink to parent record (for Attachments and ContentVersion records)	
Blackthorn Compliance__Category__c*	Text	Classification of Log.	• Record Reported • Record Deleted • Record Masked
Blackthorn Compliance__CreditCardDetected__c	Checkbox	True if credit card number is detected.	
Blackthorn Compliance__Exception__c	Checkbox	True if Blackthorn Compliance has detected an internal error - not detected PII.	
Blackthorn Compliance__Large_Description__c	Long Text	Long summary of Log event.	

Blackthorn Compliance__Object__c**	Text	Triggering SObject for Log event. Use this field to filter reports by SObject.	
Blackthorn Compliance__Field__c	Text	The Salesforce field in which Blackthorn Compliance discovered sensitive data.	
Blackthorn Compliance__Pattern__c	Text	The Detection Pattern matched in the detection.	
Blackthorn Compliance__Origin__c	Text	Apex origin of Log event	
Blackthorn Compliance_FalsePositive__c	Checkbox	A likely false positive. This field is flagged automatically by Blackthorn Compliance. You are allowed to manually check this box if you find valid false positives not caught by Blackthorn Compliance.	
Blackthorn Compliance__ConfidenceLevel__c	Formula	Our confidence in the detection event. Values can be High, Medium, or Low.	• High • Medium • Low
Blackthorn Compliance__PatternMatch__c	Checkbox	True if a detection pattern was matched.	
Blackthorn Compliance__LuhnValid__c	Checkbox	True if the number flagged passed the Luhn Algorithm.	
Blackthorn Compliance__LogType__c*	Formula	A standard set of values which can be used in reporting	• Mask • Report • Delete • Debug

*: Use either the Category field or the Log Type field to filter reports by action i.e. “Log Type = Report” to only return logs where there was a report event.

**: Use the Object field to filter reports by SObject e.g. “Case” will only show you Logs where the triggering records are Cases.

Mask Individual Records with Blackthorn Compliance Logs

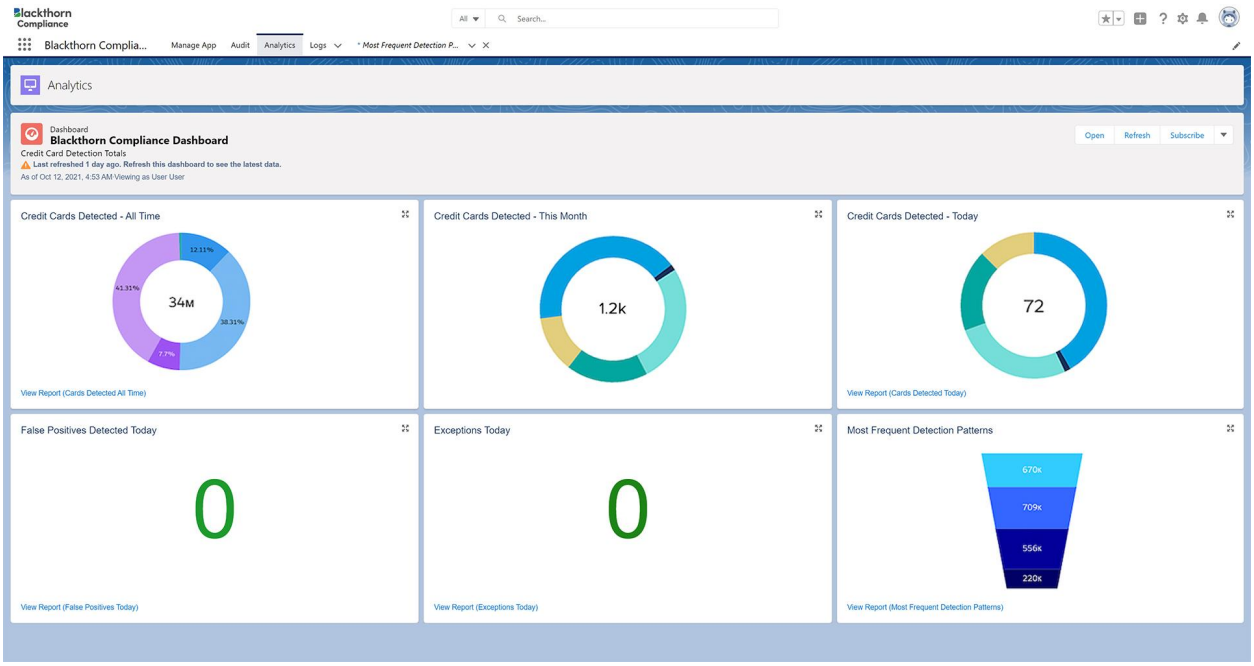


We have heard from customers that after you run a report audit, it would be nice if you could mask or delete the related record directly, instead of having to switch the audit action to mask and run the same audit again.

- We have created **Lightning Component Buttons** so you don't have run more audits just to mask a few records
- This is especially useful for customers with frequent false positives, who need an easy way for their compliance teams to manually mask the record after confirming the record does contain credit card numbers.
- These buttons are on the **Blackthorn Compliance Log page layout**, and allow your compliance team to automatically enforce PCI Compliance on one-off records directly from the Log without having to switch to the related Case, Email Message, or Attachment.
- If a credit card is masked successfully, there will be a subsequent log created for the event.

Blackthorn Compliance Dashboard

The Blackthorn Compliance Dashboard is built with the same reports in the Blackthorn Compliance Reports folder. The Blackthorn Compliance Dashboard is completely customizable - you may add more dashboard components or delete the prebuilt components. You can also create your own dashboards using the prebuilt Blackthorn Compliance Reports.



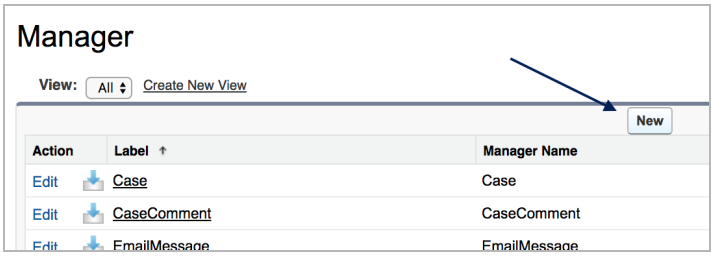
Extending Blackthorn Compliance

Extend Blackthorn Compliance to Other Objects

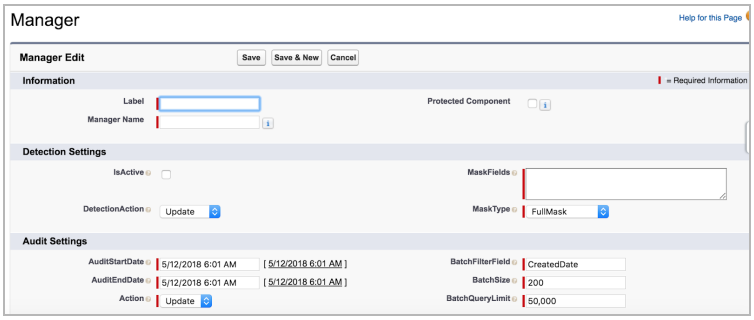
Blackthorn Compliance comes preloaded with Detection and Auditing for many standard objects, but what if you want to detect credit cards on custom objects or other standard objects?

Part One: *Create a new Manager Record*

1. Create new Blackthorn Compliance Manager Record
    a. **Setup > Custom Code > Custom Metadata Types > Manager > Manager Records > New**



2. Enter the API Name of the Object in the **Label** field (must be exact API Name)



3. Enter the Name of the Object in the **Manager Name** field (cannot contain consecutive underscores)
4. Enter the comma-delimited API names for Text fields in **Detection Fields**
    a. These fields are where Blackthorn Compliance will look for credit card numbers
5. Select a **Detection Action**
6. Press **Save**

Part Two: *Extend Blackthorn Compliance with an Apex Trigger**

* If you are running Blackthorn Compliance Audits **only**, then you can skip this step. If you don't care about new records getting processed, and are only cleaning up old records, again - you can skip this step.

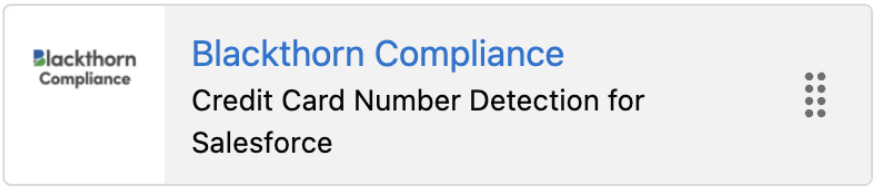
Now we'll need to get a little advanced - writing a *super easy* Apex Trigger on the Object you are extending Blackthorn Compliance to.

1. Create a new Apex Trigger for the Object:
    a. **Classic: Setup > Create > Objects > Click on the Object name > Triggers > New**
    b. **Lightning: Setup > Object Manager > Click on the Object name > Triggers > New**

2. Copy & Paste the following lines of code (replacing all "**NewHouse**" references with the API name of the Object you wish to extend Blackthorn Compliance to):

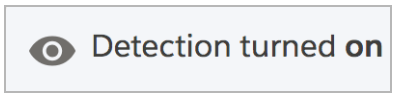
```
trigger NewHouseTrigger on NewHouse (before insert, before update) {
    if (Blackthorn Compliance.Manager.isOnline('NewHouse')) {
        Blackthorn Compliance.Processor.maskCreditCards(
            Trigger.new,
            Blackthorn Compliance.Manager.getMaskFields('NewHouse'),
            'NewHouse'
            );
    }
}
```

3. Press **Save**
4. Navigate back to the Blackthorn Compliance App



5. Turn on Detection for the Object

6. You should see the following alert notification

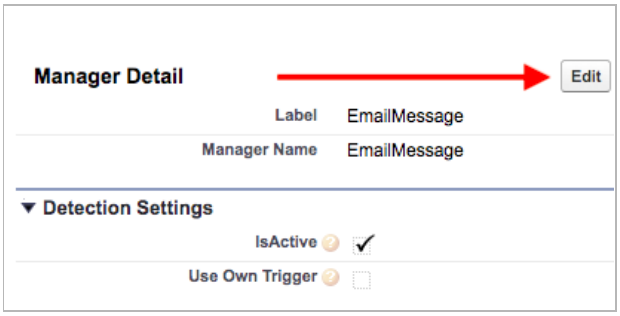


7. Congratulations! You have successfully added a new Object to Blackthorn Compliance.

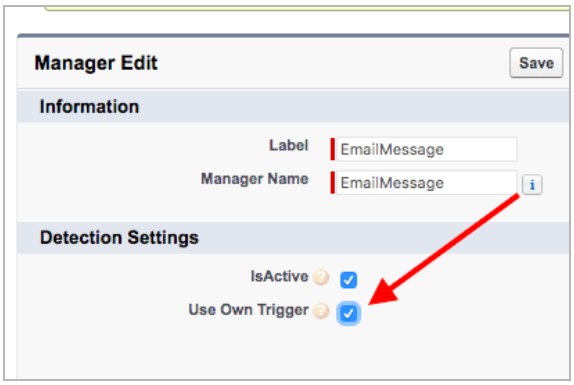
Writing Custom Blackthorn Compliance Triggers

Blackthorn Compliance comes with native Apex Triggers on standard objects included in a Blackthorn Compliance subscription. If you want to write your own triggers instead, you simply need to change a Manager Setting field. This tells Blackthorn Compliance to **NOT** execute its native triggers.

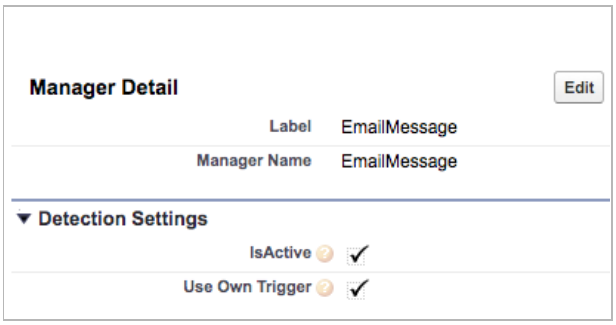
1. Navigate to the Manager Setting for the standard object
    a. Setup > Develop > Custom Metadata Types > Manager > Manage Records > Click on the object name
    b. Press **Edit**



    c. Check the box **Use Own Trigger**



    d. Press **Save**



    e. Now create your own Apex Trigger using the code snippet below as an example

Sample Custom Blackthorn Compliance Apex Trigger:

```
trigger InboundEmailMessageTrigger on EmailMessage (before insert) {
    List<EmailMessage> incomingEms = new List<EmailMessage>();

    // if Detection is turned on for Email Message
```

```
    if (Blackthorn Compliance.Manager.isOnline(Blackthorn Compliance.StaticUtils.EMAILMESSAGE)) {
        // collect incoming emails
        for (EmailMessage em : Trigger.new) {
            if (em.Incoming) {
                incomingEms.add(em);
            }
        }
        // process only incoming emails with Blackthorn Compliance
        Blackthorn Compliance.Processor.maskCreditCards(
            incomingEms,
            Blackthorn Compliance.Manager.getMaskFields(Blackthorn
Compliance.StaticUtils.EMAILMESSAGE),
            Blackthorn Compliance.StaticUtils.EMAILMESSAGE
        );
    }
}
```

Blackthorn Compliance Class Methods

List of methods you can call from the **Blackthorn Compliance** namespace

Class	Method	Parameters	Description
Blackthorn Compliance.Processor	maskCreditCards()	• records : List<SObject> • fieldNames: List<String> • objectName: String	Void method for scanning text for PII
Blackthorn Compliance.Manager	isOnline()	• objectName: String	Checks if Manager setting is online. Returns Boolean
Blackthorn Compliance.Manager	getMaskFields()	• objectName: String	Returns list of field names for a given object
Blackthorn Compliance.Manager	getDetectionAction()	• objectName: String	Returns the DetectionAction for a given object

False Positives

What is a False Positive?

A **false positive error**, or in short a **false positive**, commonly called a "**false alarm**", is a result that indicates a predicted value exists, when it does not. For example, a DLP solution might flag a credit card number, but if it turns out to be a mobile number then this is a false positive. At Blackthorn Compliance, we are conservative in enforcing PCI Compliance rules, but our algorithm also has high precision and recall, which significantly reduces the false positive rate. There are always instances where despite our best predictions, false positives squeak through. The following section explains what you should do when this happens.

Mitigating False Positives

1. Turn on **Luhn Check** for all credit card patterns.
    - Making sure the field Luhn Check is true for your credit card patterns will ensure that numbers will go through a second validation - namely verifying that the supposed credit card number passes the Luhn Algorithm.
2. **Customize** detection pattern **Regular Expressions** to be more strict.
    - You can customize the out-of-the-box RegEx that comes with Blackthorn Compliance. Consider adjusting the RegEx patterns to be more “strict” - more of an exact match for a specific pattern type.
3. **Disable** Patterns you don’t need.
    - Don’t do business overseas? Then you don’t need Maestro, JCB, and other international credit cards. Disable these patterns to significantly reduce false positives. Likewise, you don’t need to mask Social Security Numbers to be PCI compliant (that’s another story altogether).
4. Create **Negative Detection Patterns**.
    - Create patterns for USPS or Fedex tracking numbers, German phone numbers, and more frequent false positive candidates with negative patterns. These will effectively exclude known patterns from Blackthorn Compliance masking. Check out the section **Negative Detection Patterns** for more info.

5. **Flag Logs** with the **False Positive checkbox** field.
    - Did a false positive come up during production testing? Crowdsource false positive data by manually flagging logs which weren't actually a credit card. False positives found by matched Negative Patterns will be flagged automatically.

Known Limitations

Blackthorn Compliance does not officially support Detection or Audit for **Rich-Text Fields**. However, if your rich-text field does not contain inline images, then Blackthorn Compliance will still successfully detect PII.

Installation Troubleshooting

1. The user installing Blackthorn Compliance **MUST** have the User Permission *Change Dashboard Colors*.
    a. Setup > Users > Permission Set.
    b. Create new permission set for your admin. Choose License [Salesforce].
    c. Under Permission Set Overview click on System Permissions
    d. Click Edit and check **Change Dashboard Colors**
    e. Assign this permission set to the user installing Blackthorn Compliance
    f. Install Blackthorn Compliance
2. Professional Edition is **NOT** supported