# Getting Started with Fraud Alert

August 2013

CyberSource®
the power of payment

CyberSource Corporation HQ | P.O. Box 8999 | San Francisco, CA 94128-8999 | Phone: 800-530-9095

## CyberSource Contact Information

For general information about our company, products, and services, go to http://www.cybersource.com.

For sales questions about any CyberSource Service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center at http://www.cybersource.com/support.

## Copyright

© 2013 CyberSource Corporation. All rights reserved. CyberSource Corporation ("CyberSource") furnishes this document and the software described in this document under the applicable agreement between the reader of this document ("You") and CyberSource ("Agreement"). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by CyberSource. CyberSource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, You may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of CyberSource.

## Restricted Rights Legends

**For Government or defense agencies.** Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

**For civilian agencies.** Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in CyberSource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

## Trademarks

CyberSource, The Power of Payment, CyberSource Payment Manager, CyberSource Risk Manager, CyberSource Decision Manager, CyberSource Connect, Authorize.Net, and eCheck.net are trademarks and/or service marks of CyberSource Corporation. All other brands and product names are trademarks or registered trademarks of their respective owners.

# Contents

# Recent Revisions to This Document

| Release | Changes |
|---|---|
| August 2013 | This revision contains only editorial changes and no technical updates. |
| June 2013 | Initial release. |

# Getting Started with Fraud Alert

When credit card fraud is detected, card-issuing banks send the transaction details to the Fraud Alert service. Then Fraud Alert sends an email notification to you if your organization is affected by any of the reportedly fraudulent transactions. You can use this information to stop shipments, intercept already-shipped orders, or cancel orders of digital goods. You can also refund the order to avoid chargeback fees and update CyberSource Decision Manager with the alert data to prevent future fraudulent transactions.

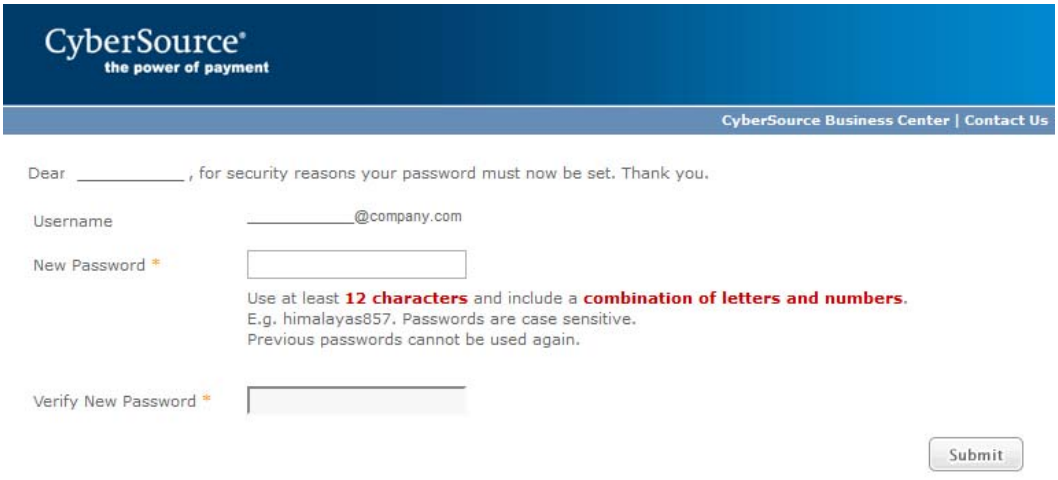
## Account Security

### Creating a Password

After CyberSource sets up your account, you receive a welcome email message that contains your username and a link.

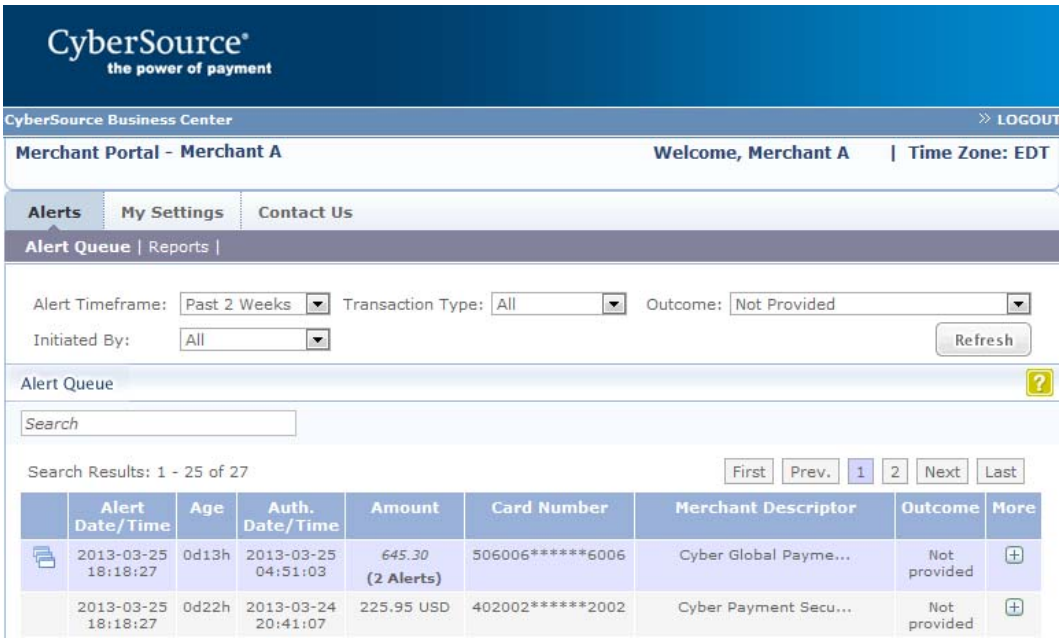
#### To set your password:

**Step 1** Click the link in the welcome email message. The set password window appears:



**Step 2** Enter your new password, and then re-enter it in the **Verify New Password** field.

**Step 3** Click **Submit**. You are logged in to the Fraud Alert portal and can view your active alerts:




# Resetting a Password

## To reset your password:

**Step 1** Navigate to www.cybersource.com/fraudalert.

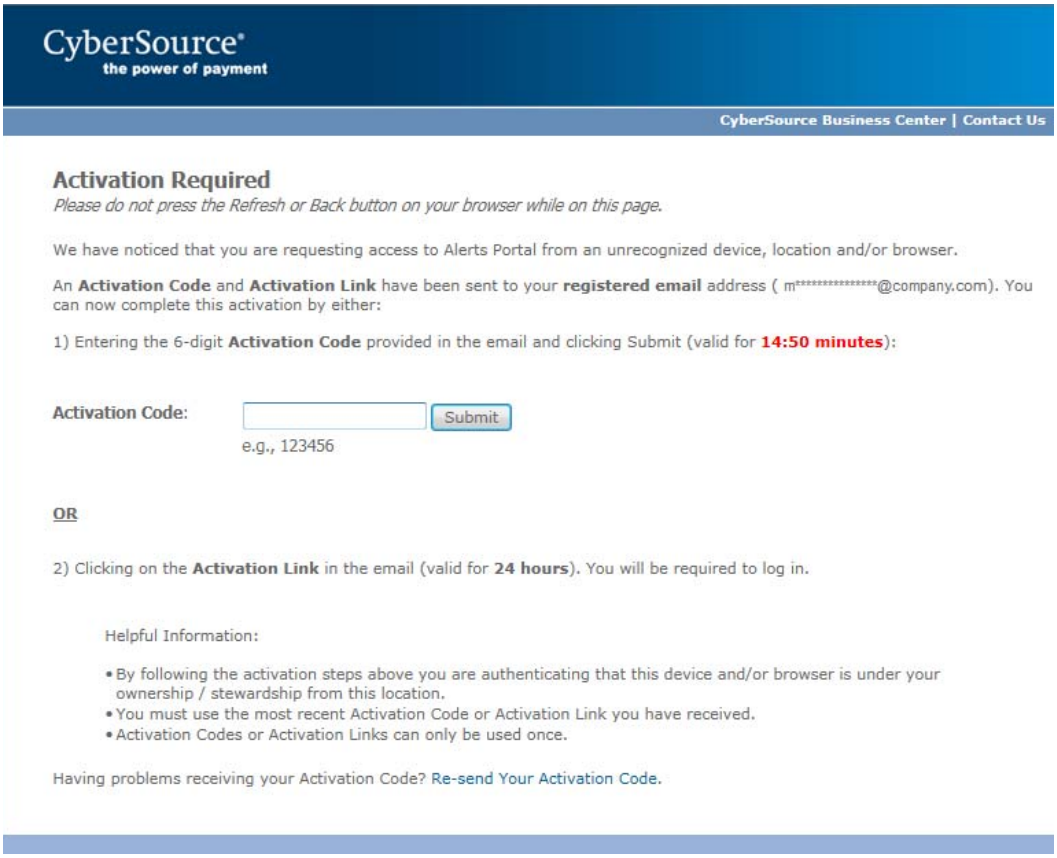
**Step 2** Click **Forgot your username or password**.

**Step 3** Enter your username, which is usually your email address.

**Step 4** Click **Submit**. When a valid username is entered, an email with reset instructions is sent to the email account associated with the username.

# Re-authenticating to the Fraud Alert Portal

The Fraud Alert portal uses IP address, operating system, and browser information in combination with the username and password to authenticate users. If any of this identifying information has changed since the last time you logged in, the Activation Required window appears when you navigate to the portal:



## To re-authenticate to the portal:

When you are redirected to the Activation Required window, an activation code is sent to the email address that is registered with your account.

**Step 1** Open the email from the Fraud Alert service.

**Step 2** Copy the 6-digit Activation Code and paste it into the **Activation Code** field in the Activation Required window. You can also click the Activation Link in the email to re-authenticate to the portal.

**Step 3** Click **Submit**. The Fraud Alert portal appears.

**Important**

- Each activation code can be used only once.
- If you enter the wrong activation code, a new code is sent to you because the initial code expires after a failed attempt to re-authenticate to the portal.
- The activation link in the email is associated with the activation code. If you enter the wrong activation code, both the code and the email link expire after a failed attempt to re-authenticate to the portal.
- Activation codes expire within 15 minutes.
- Activation links in emails are valid for 24 hours.

# Using the Fraud Alert Service

## Fraud Alert Email Notifications

Email notifications are sent for each transaction that affects your organization. Notifications can be sent to individuals or email distribution lists.

The fraud alert email notification contains your merchant account name (descriptor), the transaction amount, and the authorization date of the transaction:

From: alerts@ethoca.com [mailto:alerts@ethoca.com]
Sent: Thursday, April 10, 2013 7:29 AM
To: Recipient
Subject: CyberSource Fraud Alert (Amount: 920.10 USD)

**Dear CyberSource Merchant,**

You have a new CyberSource Fraud Alert.

Merchant descriptor: Cybersource Merchant ABC
Amount: 920.10 USD
Auth Date: 09 April 2013

Please login to the CyberSource Fraud Alert portal today to see the details of the fraudulent transaction and update your system.
LOGIN ://www.cybersource. ethoca.com/

Sincerely,

**CyberSource**

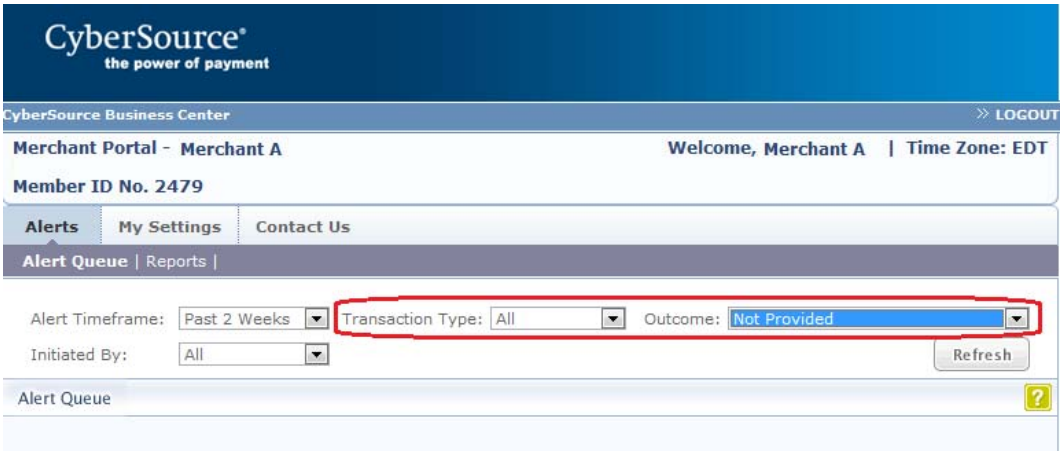
# Responding to Fraud Alerts

## To respond to fraud alerts:

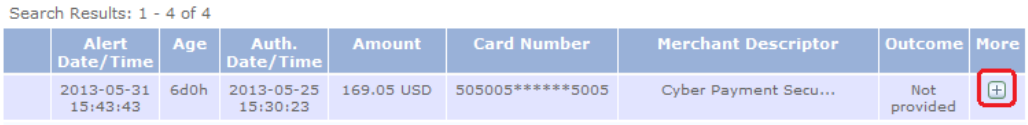
**Step 1** In the fraud alert email notification, click **LOGIN://www.cybersource.ethoca.com/**. The Fraud Alert portal login page appears.

**Step 2** Enter your username and password, and then click **Login**.

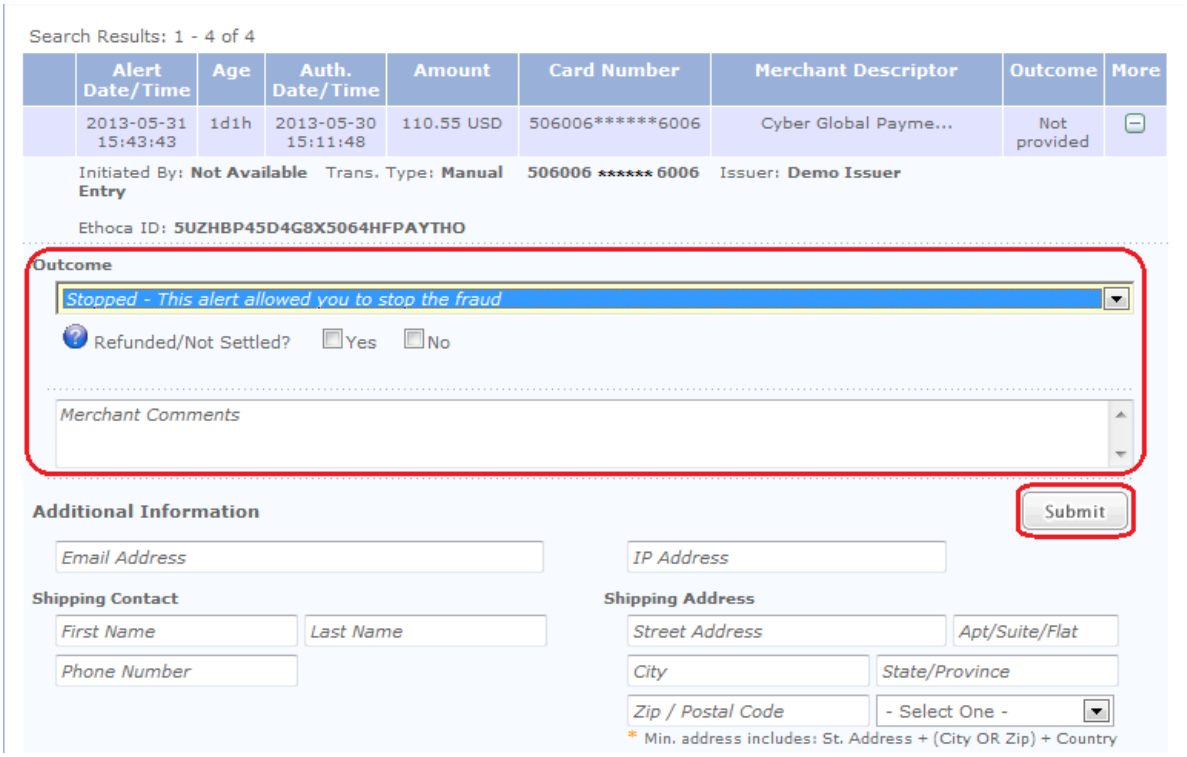
**Step 3** In the Fraud Alert portal, adjust the filters at the top of the window to ensure that you are capturing all alerts. Outcome: Not Provided appears the first time that you log in. It ensures that all alerts that require a response are displayed:




**Step 4** Click the plus sign in the More column of Search Results to expand the alert and review additional transaction information:



**Step 5** Choose an outcome from the drop-down list.




**Important**

Providing the Outcome enables the card-issuing bank to identify additional fraud and send additional alerts to you.

**Step 6** Check **Yes** if your organization is processing a refund or is not settling the transaction. Check **No** if your organization is disputing the chargeback.

**Step 7** Under **Additional Information**, you may choose to enter an email address, IP address, or contact and shipping information.

**Step 8** Click **Submit** to upload the information to the Fraud Alert service.

# Using the Fraud Alert Service with Decision Manager

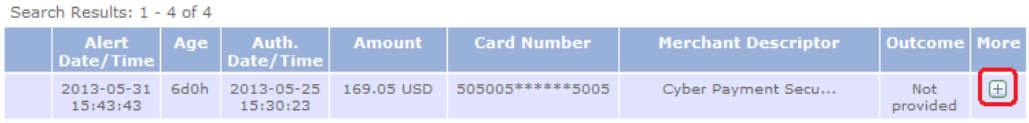
When you receive fraud alert email notifications, you can log in to the Fraud Alert portal, copy the card account number, and search for it in the Decision Manager Case Search window. Then you can update CyberSource Decision Manager with the alert data to prevent future fraudulent transactions. For more information about logging in to the Fraud Alert portal, see "Responding to Fraud Alerts," page 10.

## To use the fraud alert service with Decision Manager:

**Step 1** Log in to the Fraud Alert portal.

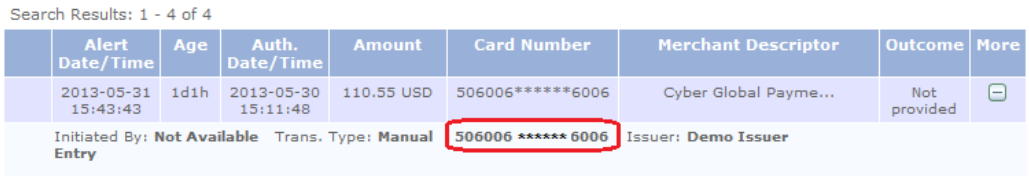
**Step 2** In the Fraud Alert portal, adjust the filters at the top of the window to ensure that you are capturing all alerts.

**Step 3** Click the plus sign in the More column of Search Results to expand the alert and view the card account number:


Search Results: 1 - 4 of 4

| | Alert Date/Time | Age | Auth. Date/Time | Amount | Card Number | Merchant Descriptor | Outcome | More |
|---|---|---|---|---|---|---|---|---|
| | 2013-05-31 15:43:43 | 6d0h | 2013-05-25 15:30:23 | 169.05 USD | 505005******5005 | Cyber Payment Secu... | Not provided | ⊞ |

**Step 4** In the expanded Search Results pane, copy the card account number:


Search Results: 1 - 4 of 4

| | Alert Date/Time | Age | Auth. Date/Time | Amount | Card Number | Merchant Descriptor | Outcome | More |
|---|---|---|---|---|---|---|---|---|
| | 2013-05-31 15:43:43 | 1d1h | 2013-05-30 15:11:48 | 110.55 USD | 506006******6006 | Cyber Global Payme... | Not provided | ⊟ |

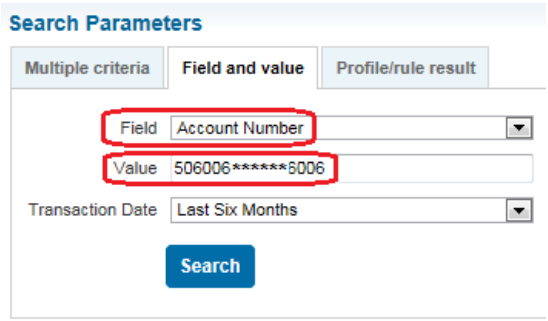
Initiated By: **Not Available** Trans. Type: **Manual Entry** **506006 ****** 6006** Issuer: **Demo Issuer**

**Note** The credit card number has been blocked in the preceding illustration, but the full account number appears on the Fraud Alert portal.

**Step 5** Log in to the Business Center.

**Step 6** From the Business Center home page, choose **Decision Manager > Case Search**.

**Step 7** In the Decision Manager Case Search window, go to the Search Parameters pane and choose the **Field and value** tab:




**Step 8** Choose **Account Number** from the Field drop-down list.

**Step 9** Paste the card account number that you copied in Step 4 into the Value field.

**Step 10** Choose a transaction date from the drop-down list.

**Step 11** Click **Search**.

---

When you find transactions associated with the card number, you can review them to determine which transaction matches the date and amount specified by the Fraud Alert portal. Then examine any other transactions involving the credit card to ensure they are not fraudulent. To ensure that additional transactions involving the compromised card are not processed, you can add the card number information to your negative customer list.

For more information about using Decision Manager, see the *CyberSource Decision Manager User Guide* in the Business Center.

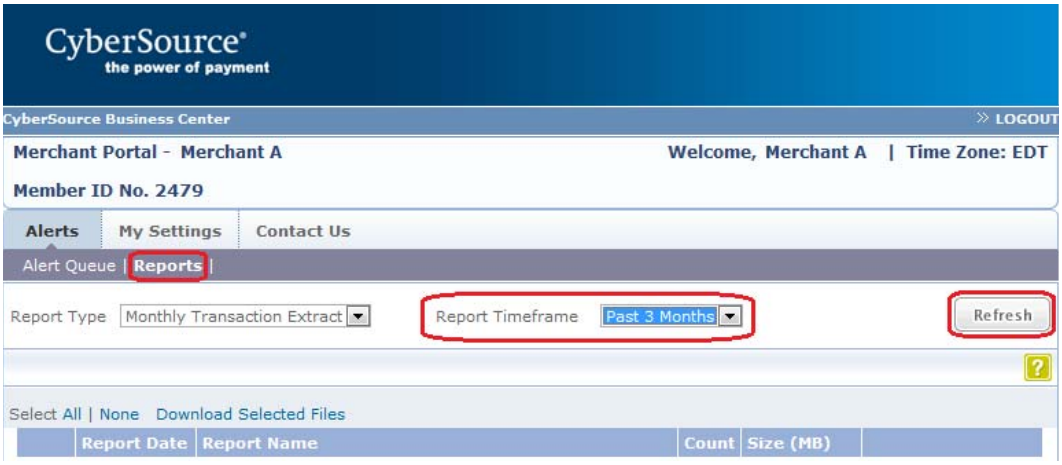
# Downloading Reports

You can download monthly transaction reports for three-month, six-month, or one-year time periods. For more information about logging in to the Fraud Alert portal, see "Responding to Fraud Alerts," page 10.

## To download monthly transaction reports:

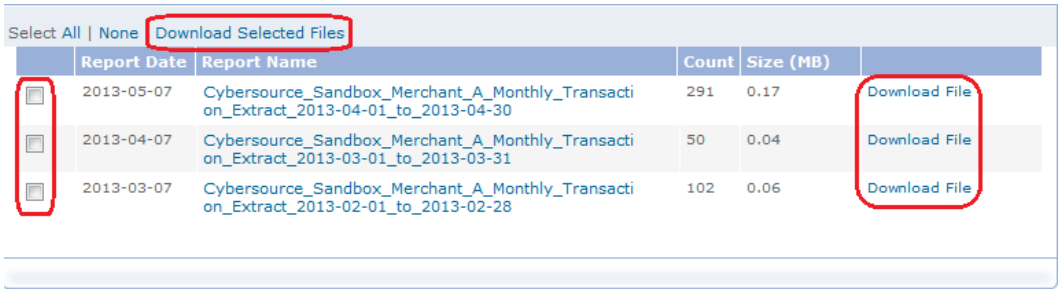
**Step 1** Log in to the Fraud Alert portal.

**Step 2** Click **Reports**:




**Step 3** Choose a report time period from the **Report Timeframe** drop-down list, and click **Refresh**. You can choose from Past 3 Months, Past 6 Months, or Past Year.

**Step 4** Check boxes in the left-most column to choose reports to download.




**Step 5** Click **Download Selected Files**. To download only one file, click **Download File**.

Use Microsoft Excel to open the report file.