

This report guide provides an overview of the information contained in the different sections of the reports generated by Restaurant Guard.

## Alert Report Overview

All Restaurant Guard Alert Reports have the same general format which is described below.

**1** Report Header

**2** Alert Information

**3** Alert Description

**4** Alert Detail

**5** Recent Incidents

**6** Incident History

**7** Report Footer

<b>1</b>	<b>Report Header</b> — Displays the company name, employee ID, and report generation date.
<b>2</b>	<b>Alert Information</b> — Identifies the suspicious employee ID and the name associated with that ID as well as the store ID and store name where the transactions occurred. Also identifies the type of suspicious event being reported.
<b>3</b>	<b>Alert Description</b> — Presents a narrative description of the type of suspicious event being reported; typically includes an overview of the scam as well as an example.
<b>4</b>	<b>Alert Detail</b> — Provides a detailed account of a recent example of this suspicious event type performed by the subject employee. This detail will include the date of the event and all transactions that identify this event as suspicious as well as any additional information that may be considered when generating the report.
<b>5</b>	<b>Recent Incidents</b> — Displays each event of the report's suspicious event type that has occurred within the reporting period. Example: if the company was on a weekly reporting cycle, the Recent Incidents section of the report above would display all Transfer events that have happened in the last week
<b>6</b>	<b>Incident History</b> — Displays a summary of all alerts for the report's subject employee ID. This section will not only display a summary for the report alert type (Transfer in the example above), but will also show a summary for any other alerts that have been generated for this employee ID.
<b>7</b>	<b>Report Footer</b> — Displays the Restaurant Guard legal disclaimer and page number.

**DISCLAIMER:** While Restaurant Guard Alerts provide analysis of transaction records based on transaction patterns and activity that are consistent with indicia of fraudulent transaction schemes that commonly occur in hospitality operations, the patterns and activities reported by Restaurant Guard may not necessarily be the result of fraudulent activity and the use of Restaurant Guard's results and analysis should be done with caution and the exercise of careful judgment. The use of Restaurant Guard and its results is subject to the disclaimers, limitations and indemnities contained in the terms and conditions for this application, which may be accessed at [www.restaurantguard.com](http://www.restaurantguard.com).

**Transfer Scam Alert Report**

A Transfer Scam Alert follows the general Alert Report format and is generated for an employee when any of their transactions exhibit suspicious transfer activity..

**Alert Description**

The Transfer or Wagonwheel Scam typically involves transferring self service items (those that don't generate a kitchen chit), such as coffee or soda, off of a check that has been paid for with cash and reusing the same item on another check.

Example:

- A guest orders a soda and sandwich and is presented a check with both items.
- The guest pays for the check with cash.
- The server transfers the soda to another check and then closes the check with only the sandwich remaining to cash, pocketing the difference.
- The check with the transferred soda is then used for the server's next table.

Employees engaging in this activity will often transfer the same item multiple times; each time the item is successfully transferred from a cash check results in a sales loss for the restaurant and a fraudulent cash gain for the server.

**Alert Detail**

The Alert Detail section of the Transfer Scam Alert will display every transfer transaction that involves the suspicious item. The section will also include the order time of the item and the open time of the first check, as well as the close time and tender transactions for every check to which the item was transferred.

**Recent Events**

<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>
Date	Item	First Check	Last Check	# Transfers	Item Price	Potential Loss
02/07/2009	Soft Drink	1001	2032	2	1.79	3.58
02/07/2009	Iced Tea	1046	3012	5	1.79	8.95
02/07/2009	Iced Tea	1005	1014	3	1.79	5.37
02/05/2009	Coffee	2210	2215	2	1.59	3.18
02/05/2009	Iced Tea	1114	1154	3	1.79	5.37
02/05/2009	Soft Drink	3100	1146	6	1.79	10.74
02/05/2009	Soft Drink	1111	1121	2	1.79	3.58
02/05/2009	Soft Drink	1102	1146	4	1.79	7.16

<b>1</b>	<b>Date</b> — The date of the suspicious event.
<b>2</b>	<b>Item</b> — The item exhibiting the suspicious transfer activity.
<b>3</b>	<b>First Check</b> — The check that the item was initially added to, and the first check in the transfer chain.
<b>4</b>	<b>Last Check</b> — The last check the item was on when the check was closed. Occasionally the first and last check numbers will be the same; this means that the item was transferred back to the check where it was initially rung up and then that check was closed.
<b>5</b>	<b># Transfers</b> — The number of times the item was transferred. A transfer is considered any activity that results in the item being assigned to a new check number; this can include: a self transfer, a split check or an add tab and any other activity that will cause the item's check number to change.
<b>6</b>	<b>Item Price</b> — The price of the item.
<b>7</b>	<b>Potential Loss</b> — Displays the potential loss in revenue to the restaurant caused by the event.

DISCLAIMER: While Restaurant Guard Alerts provide analysis of transaction records based on transaction patterns and activity that are consistent with indicia of fraudulent transaction schemes that commonly occur in hospitality operations, the patterns and activities reported by Restaurant Guard may not necessarily be the result of fraudulent activity and the use of Restaurant Guard's results and analysis should be done with caution and the exercise of careful judgment. The use of Restaurant Guard and its results is subject to the disclaimers, limitations and indemnities contained in the terms and conditions for this application, which may be accessed at [www.restaurantguard.com](http://www.restaurantguard.com).

## Void after Close Alert Report

A Void after Close Alert follows the general Alert Report format and is generated for an employee when any of their transactions exhibit suspicious void after close activity.

### Alert Description

The Void after Check Close Scam is typically performed by management at the restaurant and has a fairly simple premise:

- The manager finds a check closed to cash by an employee who has already checked out.
- The manager reopens the check, voids some or all of the items and then closes the check again.

Because the employee has already checked out, they have turned in cash equal to the amount of the check before the items were voided. After the items are voided a cash over situation is created, and this difference is pocketed by the manager.

### Alert Detail

The Alert Detail section of the Void after Close Alert contains the initial check close time, check reopen time, any tender (apply or delete) transactions associated with the check and the items voided. Each transaction will display the check employee and authorizing manager when available.

### Recent Events

①	②	③	④	⑤	⑥
Date	Check Number	Check Employee	Minutes after Close	# Items Voided	Potential Loss
3/14/2009	1001	101 (Beltz, Chuck)	225	4	38.99
3/12/2009	2101	152 (Magee, Bill)	186	3	26.28
3/11/2009	1115	101 (Beltz, Chuck)	291	5	42.99
3/10/2009	3006	123 (Henriksen, Charles)	308	6	40.70
3/9/2009	2054	111 (Hughes, Jason)	94	3	34.99

①	<b>Date</b> — The date of the suspicious event.
②	<b>Check Number</b> — The check exhibiting the suspicious void after close activity.
③	<b>Check Employee</b> — The employee who owned the check at the time of the suspicious void.
④	<b>Minutes after Close</b> — The amount time, in minutes, after the check was initially closed that the suspicious void was performed.
⑤	<b># Items Voided</b> — The number of items voided from the check after it was initially closed.
⑥	<b>Potential Loss</b> — Displays the potential loss in revenue to the restaurant caused by the event.

## Comp after Close Alert Report

A Comp after Close Alert follows the general Alert Report format and is generated for an employee when any of their transactions exhibit suspicious comp after close activity.

### Alert Description

The Comp after Check close Scam is typically performed by management at the restaurant and has a fairly simple premise:

- The manager finds a check closed to cash by an employee who has already checked out.
- The manager reopens the check, applies a comp and then closes the check again.

Because the employee has already checked out, they have turned in cash equal to the amount of the check before the comp was applied. After the comp is applied a cash over situation is created, and this difference is pocketed by the manager.

### Alert Detail

The Alert Detail section of the Comp after Close Alert contains the initial check close time, check reopen time, any tender (apply or delete) transactions associated with the check and the comp(s) applied. Each transaction will display the check employee and authorizing manager when available.

### Recent Events

①	②	③	④	⑤	⑥
Date	Check Number	Check Employee	Minutes after Close	Comp Name	Potential Loss
02/05/2009	2100	125 (Beltz, Charles)	276	Promo 100%	42.38
02/03/2009	1005	121 (Sullivan, Jason)	290	Mgr Comp	23.98
02/03/2009	1034	125 (Beltz, Charles)	187	Promo 100%	36.25
02/02/2009	3152	134 (Henriksen, Chuck)	226	Promo 100%	19.42
02/02/2009	1254	134 (Henriksen, Chuck)	281	Mgr Comp	29.81

①	<b>Date</b> — The date of the suspicious event.
②	<b>Check Number</b> — The check exhibiting the suspicious comp after close activity.
③	<b>Check Employee</b> — The employee who owned the check at the time of the suspicious comp.
④	<b>Minutes after Close</b> — The amount time, in minutes, after the check was initially closed that the suspicious comp was performed.
⑤	<b>Comp Name</b> — The name of the comp that was applied to the check after it was reopened.
⑥	<b>Potential Loss</b> — Displays the potential loss in revenue to the restaurant caused by the event.

**Comp after Print Alert Report**

A Comp after Print Alert follows the general Alert Report format and is generated for an employee when any of their transactions exhibit suspicious comp after print activity.

**Alert Description**

A Comp after Print Check can be an indicator that an employee is engaging in fraudulent activity.

When performed as part of a scam, the employee will print a check for the full amount and present it to the customer. After the customer pays cash for the bill, the employee has a comp applied to the check and keeps what the customer paid in cash and the total after the comp for themselves. The check is typically not printed again after the comp is applied.

Example:

- A guest orders a soda, burger and side of fries and receives all of the items.
- The check is printed and the guest is presented with a bill for all of the items.
- The guest pays for the check with cash.
- The server has the side of fries comped off of the check, telling the manager that the guest didn't like them.
- The server pockets the value of the comped side of fries.

Employees engaging in this activity will often approach a manager when they are busy and ask to borrow their card to comp an item for an unhappy guest.

**Alert Detail**

The Alert Detail section of the Comp after Print Alert will display the time the check was opened, the amount of the check before the comp, each time the check was printed, the comp(s) applied to the check and when and to which tender the check was closed.

**Recent Events**

①	②	③	④	⑤
Date	Check Number	Comp Name	Manager	Potential Loss
02/02/2009	2100	Walk	901 (Jones, Lisa)	16.40
02/02/2009	1005	Made Wrong	901 (Jones, Lisa)	4.99
02/01/2009	1101	Didn't Like	910 (Hughes, Jason)	13.99
02/01/2009	2054	Made Wrong	910 (Hughes, Jason)	6.49
01/28/2009	3015	Walk	901 (Jones, Lisa)	22.34

①	<b>Date</b> — The date of the suspicious event.
②	<b>Check Number</b> — The check exhibiting the suspicious comp after print activity.
③	<b>Comp Name</b> — The name of the comp applied to the check after the print.
④	<b>Manager</b> — The manager who approved the comp transaction.
⑤	<b>Potential Loss</b> — Displays the potential loss in revenue to the restaurant caused by the event.

DISCLAIMER: While Restaurant Guard Alerts provide analysis of transaction records based on transaction patterns and activity that are consistent with indicia of fraudulent transaction schemes that commonly occur in hospitality operations, the patterns and activities reported by Restaurant Guard may not necessarily be the result of fraudulent activity and the use of Restaurant Guard's results and analysis should be done with caution and the exercise of careful judgment. The use of Restaurant Guard and its results is subject to the disclaimers, limitations and indemnities contained in the terms and conditions for this application, which may be accessed at [www.restaurantguard.com](http://www.restaurantguard.com).

**Over Tip Alert Report**

An Over Tip Alert follows the general Alert Report format and is generated for an employee when the number of Over Tips they receive becomes significantly greater than the average employee. An Over Tip is defined as any tip greater than 30% of the check total.

**Alert Description**

The Over Tip scam has a simple premise: the bartender or server gives away self service items, such as a drink in the bar or a dessert in the restaurant, to a guest with the expectation of receiving a larger than normal tip.

Example:

- A guest sits down at the bar and over the course of two hours orders five beers.
- When the guest is ready to leave they are presented with a check that has only one beer. The bartender hasn't run up any of the other beers they've given to the guest.
- The guest leaves a \$20 tip on their \$5 tab to thank the bartender for the free beers.
- The 400% tip is significantly larger than the typical 18% tip at this bar and is considered an Over Tip by Restaurant Guard.

A bartender or server receiving a significantly more than average number of Over Tips can signify that the employee is engaging in the Over Tip scam.

Note: Restaurant Guard analyses only credit card tips for the Over Tip Alert.

**Alert Detail**

The Alert Detail section of the Over Tip Alert contains the statistics regarding the site's average tip % and the number of High Tips the employee receives as compared to the average employee. The section also displays a chart displaying the relationship of the subject employees tips versus the average employee.

**Recent Events**

①	②	③	④	⑤	⑥
Date	Check Number	Check Amount	Tip Amount	Tip %	Potential Loss
3/12/2009	50037	\$1.00	\$50.00	5000.00%	\$41.82
3/11/2009	50016	\$10.00	\$50.00	500.00%	\$49.20
3/12/2009	50027	\$5.00	\$25.00	500.00%	\$24.60
3/17/2009	50014	\$5.00	\$25.00	500.00%	\$24.60
3/6/2009	50050	\$15.00	\$60.00	400.00%	\$61.50
3/12/2009	50001	\$5.00	\$20.00	400.00%	\$20.50

①	<b>Date</b> — The date of the suspicious event.
②	<b>Check Number</b> — The check receiving the High Tip.
③	<b>Check Amount</b> — The amount of the check when it was closed.
④	<b>Tip Amount</b> — The amount of the tip left on the check.
⑤	<b>Tip %</b> — The percentage of the tip as compared to the check amount – [Tip Amount] divided by [Check Amount].
⑥	<b>Potential Loss</b> — Displays the potential loss in revenue to the restaurant caused by the event.

DISCLAIMER: While Restaurant Guard Alerts provide analysis of transaction records based on transaction patterns and activity that are consistent with indicia of fraudulent transaction schemes that commonly occur in hospitality operations, the patterns and activities reported by Restaurant Guard may not necessarily be the result of fraudulent activity and the use of Restaurant Guard's results and analysis should be done with caution and the exercise of careful judgment. The use of Restaurant Guard and its results is subject to the disclaimers, limitations and indemnities contained in the terms and conditions for this application, which may be accessed at [www.restaurantguard.com](http://www.restaurantguard.com).

**Employee Rankings Detail Report**

The Employee Rankings Detail Report ranks all employees across several different categories using normalized data. A lower number in a ranking category means that an employee is performing well in that category while a higher number means that the employee is performing poorly; an employee with a ranking of 1 is performing as good as or better than all other employees in that category.

		2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Employee Rankings Detail View	Store	Overall Score	Total Checks	Check Time Avg Rank	Tip Avg Rank	Drink Sales Avg Rank	Drink Items Avg Rank	Add-On Sales Avg Rank	Add-On Sales Items Rank	Comp Avg Rank	Check Total Avg Rank	Void Avg Rank	Clear Avg Rank	FRAUD INDEX RANK
1	Puckett, David	30th Street Marketplace	28.2	1163	86	50	7	11	43	33	29	13	1	29	28
2	Monge, Lisa	Willowbrook	28.5	1935	91	128	2	1	3	2	16	1	1	97	36
3	Nunez, David	30th Street Marketplace	30.2	5313	106	105	3	12	42	40	26	5	1	21	6
4	Fritsch, Laura	Willowbrook	31.6	1384	115	20	18	4	2	3	85	4	118	90	10
	Stuchlik, Robert	Century City	37.2	8194	74	35	25	20	29	26	50	2	53	9	21

1	<b>Employee Name and Overall Rank</b> — The overall rank and name of the employee.
2	<b>Store</b> — The name of the store where the employee works.
3	<b>Overall Score</b> — A weighted average of the scores from each of the other categories on the report.
4	<b>Total Checks</b> — The total number of the employee's checks analyzed by Restaurant Guard
5	<b>Check Time Avg Rank</b> — The ranking of the average check (turn) time for the employee's checks; lower average check times are ranked better.
6	<b>Tip Avg Rank</b> — The ranking of the average tip % for the employee's checks; a higher average tip % is considered good
7	<b>Drink Sales Avg Rank</b> — The ranking of the average drink sales per check for the employee. Drink items are any beverages sold in the restaurant including both alcoholic and non-alcoholic.
8	<b>Drink Items Avg Rank</b> — The ranking of the average number of beverages sold per check for the employee. Drink items are any beverages sold in the restaurant including both alcoholic and non-alcoholic.
9	<b>Add-On Sales Avg Rank</b> — The ranking of the average add-on sales per check for the employee. Add-ons include appetizers, desserts and any other a la carte items that wouldn't be considered an entrée.
10	<b>Add-On Sales Items Avg Rank</b> — The ranking of the average number of add-ons sold per check by the employee. Add-ons include appetizers, desserts and any other a la carte items that wouldn't be considered an entrée.
11	<b>Comp Avg Rank</b> — The ranking of the average comp dollars per check for the employee; lower average comps per check are ranked better.
12	<b>Check Total Avg Rank</b> — The ranking of the average check total for the employee; higher check totals are ranked better.
13	<b>Void Avg Rank</b> — The ranking of the average void dollars per check for the employee; lower average voids per check are ranked better.
14	<b>Clear Avg Rank</b> — The ranking of the average number clear dollars per check performed by the employee; a poor ranking in this category may suggest the employee is repeatedly making mistakes while ringing in checks and could point to the need for additional training on the point of sale.
15	<b>FRAUD INDEX RANK</b> — A separate index ranking performed by Restaurant Guard to gauge the employee's potential that they may be engaging in fraudulent activity. This index is computed using the data in this report as well as other metrics internal to Restaurant Guard. A poor ranking, or high number, in this index may not correspond directly to the number of Alert Reports generated for this employee.

DISCLAIMER: While Restaurant Guard Alerts provide analysis of transaction records based on transaction patterns and activity that are consistent with indicia of fraudulent transaction schemes that commonly occur in hospitality operations, the patterns and activities reported by Restaurant Guard may not necessarily be the result of fraudulent activity and the use of Restaurant Guard's results and analysis should be done with caution and the exercise of careful judgment. The use of Restaurant Guard and its results is subject to the disclaimers, limitations and indemnities contained in the terms and conditions for this application, which may be accessed at [www.restaurantguard.com](http://www.restaurantguard.com).