# Table Of Contents

1. Introduction .................................................................................. 3
2. Risk Entities .................................................................................. 3
3. View/Create/Edit Risk Settings. .......................................................... 4
   3.1. Creating a new rule ........................................................................ 5
      3.1.1. Maximum Shares per order ............................................................ 5
      3.1.2. Maximum Notional Value per order ................................................... 5
      3.1.3. Percentage of Symbol Average Daily Volume ....................................... 6
      3.1.4. Order Type/Attribution Restrictions .................................................. 7
      3.1.5. Restricted Stock List ........................................................................... 8
      3.1.6. Hard to Borrow List ........................................................................... 8
      3.1.7. Market Impact Check ......................................................................... 9
      3.1.8. Fat Finger Protection ......................................................................... 9
      3.1.9. Order Rate Thresholds ........................................................................ 10
         3.1.9.1. Duplicative Order Protection ......................................................... 10
         3.1.9.2. Message Rate Thresholds ............................................................... 11
      3.1.10. Gross Exposure - Open, Executed, Notional ...................................... 11
   3.2. Deleting a rule ............................................................................. 13
   3.3. View/Edit current rules .................................................................... 13
   3.4. Audit rules .................................................................................... 14
   3.5. Email alerts .................................................................................. 15
4. Breach and Exposure Monitoring ..................................................... 17
   4.1. Breach Monitoring .......................................................................... 17
   4.2. Exposure Monitoring ...................................................................... 18
   4.3. Safety Switch ................................................................................ 18
5. Permissioning and Configurability .................................................... 19
   5.1. Availability and Permissioning .......................................................... 19
   5.2. Configurability ............................................................................. 19

Document History. .............................................................................. 20
1. Introduction

Nasdaq offers members and sponsored access firms configurable pre-trade risk checks via a user interface on Nasdaq's WorkX platform. In addition to the configuration of risk parameters, members will also be able to monitor exposure, configure alerting, and retrieve audit information via the UI.

The risk checks are available on all order entry protocols on Nasdaq, BX, and PSX:

- OUCH
- FLITE
- FIX
- RASHport

Please note that Exchanges do not guarantee that the controls are sufficiently comprehensive to be the exclusive means by which a member can satisfy its compliance obligations under the Market Access Rule and each Exchange's market access-related rules. Furthermore, the member, and not the Exchanges, retains full responsibility for complying with such regulatory requirements. Members with market access must perform their own appropriate due diligence to assure the controls are reasonably designed to be effective, and otherwise consistent with the Market Access Rule. The SEC has stated that broker-dealers may not rely merely on representations of the technology provider, even if an exchange or other regulated entity, to meet this due diligence standard. It is the responsibility of the participant to use due diligence to assure that its risk controls are reasonably designed to be consistently and reliably effective and to periodically test the risk tools to ensure they are operating properly and effectively, and to promptly notify Nasdaq of any outage or issues the participant detects, to the extent that Nasdaq does not first affirmatively provide such notice to the participant.

2. Risk Entities

A Risk Entity is a business unit for which different risk limits may be set. The available Risk Entities and their applicability per risk control type is as follows:

- **MPID**
  - Mandatory for all checks

- **MPID + Port**
  - Entering firms have the ability to segment risk at a more detailed level by specifying a MPID + Port combination.
  - MPID + Port is required for Message Rate Threshold and Duplicative Order Protection checks

- **MPID + Symbol**
  - Entering firms will be required to specify a symbol in order to enable certain risk checks

- **MPID + Port + Symbol**
  - Entering firms have the ability to segment risk at a more detailed level by specifying a Port with the MPID + Symbol hierarchy.

- **MPID + Group ID hierarchy**
  - Entering firms have the ability to register Group IDs within their MPIDs to segment risk at a more detailed level than MPID
  - Group ID format:
    - 2 byte short integer
### Risk Control

<table>
<thead>
<tr>
<th>Risk Control</th>
<th>MPID</th>
<th>MPID + Port</th>
<th>MPID + Group ID</th>
<th>MPID + Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Notional Value per order</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Shares per order</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single Order - Percentage of Symbol ADV</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject ISO</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject Short Sale Orders</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject Non-Auction Market Orders</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject Pre-Market Trading</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject Post-Market Trading</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject Short Sale Exempt</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Require Locate</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted Stock List</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Hard to Borrow List</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Fat Finger Protection</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Market Impact Check</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Rate Threshold - Port &amp; Symbol</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Duplicative Order Protection</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Gross Exposure – Open</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Gross Exposure – Executed</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Gross Exposure - Notional</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

### 3. View/Create/Edit Risk Settings

All rule creation, maintenance, auditing, and alerts can be managed in the EQRC Rules section of the Settings menu.
3.1. Creating a new rule

- To add a new rule, select the applicable risk setting tab and click the “New Rule” button.

- Mandatory fields will be designated with an orange circle
- Newly configured rules will automatically default to a status of CONFIGURED and will not become active until the next trading session.

3.1.1. Maximum Shares per order

**Breach Action:** triggered when calculation > limit. Order rejected on arrival.

**Calculation:**
- Value specified in Shares field of the order.

**Configuration:** configurable at the MPID and MPID+Port level.
- Min: 0 Max 999,999

**Design:** Each individual order that would exceed the configured limit will be rejected on arrival.

3.1.2. Maximum Notional Value per order

**Breach Action:** triggered when calculation > limit. Order rejected on arrival.

**Calculation:**
- Calculated as booked price x Shares.

**Configuration:** configurable at the MPID level.
- Min: 0 Max: Max Long
**Design:** Each individual order that would exceed the configured limit will be rejected on arrival.

![Create Max Notional Order Rule](https://example.com)

### 3.1.3. Percentage of Symbol Average Daily Volume

**Breach Action:** triggered when Shares > calculated maximum quantity. Order rejected on arrival.

**Calculation:**

- The single order maximum quantity for a given symbol is calculated as the symbol's 20 day Average Daily Volume × the configured percentage limit.
- Additional ability for customers to specify a minimum CADV value; e.g minimum 20 day CADV is ≥ Y shares.
  - For any symbol that has a 20 day CADV below this value, the value specified by the customer will be used for calculation.
- The rolling 20-day consolidated Average Daily Volume (ADV) is updated for each symbol at the end of each trading day. If a symbol has been trading for less than 20 days, the exchange will take the average volume across the days that it has been trading. If no trading has occurred the value will be zero.

**Configuration:** configurable at the MPID and MPID+Port level.

- Min: 0% Max: 100%

**Design:**

- Each individual order that would exceed the configured limit will be rejected on arrival.
- Enabling this setting will result in this check being done on all symbols (i.e. there will not be an ability to enable on a per symbol basis).
3.1.4. Order Type/Attribution Restrictions

**Breach Action:** Order rejected on arrival.

**Configuration:** configurable at the MPID and MPID+Port level

- Reject ISO - on/off
- Reject Pre-Market Trading - on/off
- Reject Post-Market Trading - on/off
- Reject Short Sale orders – on/off
- Reject Non-Auction Market Orders – on/off
- Require Locate on Sell Short orders - on/off.
  - Applicable to orders with Side = Sell Short
  - Check only available on OUCH 5.0, FIX, and RASHport 1.2
- Reject Short Sale Exempt Orders – on/off

**Design:** Each individual order subject to the configured restriction will be rejected on arrival.
3.1.5. **Restricted Stock List**

**Breach Action:** Order rejected on arrival.

**Configuration:** configurable at the MPID+Symbol and MPID+Port+Symbol level
- Reject Restricted Symbol (all Sides) - on/off

**Design:** Each individual order subject to the configured restriction will be rejected on arrival.

![Create Restricted Stock Rule Image]

3.1.6. **Hard to Borrow List**

**Breach Action:** Order rejected on arrival.

**Configuration:** configurable at the MPID+Symbol and MPID+Port+Symbol level
- On/off

**Design:**
- Short Sale exempt orders are NOT included in this check
- Each individual order subject to the configured restriction will be rejected on arrival.

![Create Short Sale Rule Image]
3.1.7. Market Impact Check

**Breach Action:** order rejected on arrival, or cancellation when applied to a previously entered order.

**Calculation:** far-side of the current LULD bands (i.e. buy (sell) order cannot be more aggressive than the upper (lower) band).

**Configuration:** configurable at the MPID and MPID+Port level

- On/off

**Design:**

- Each individual order that would exceed the configured limit will be rejected.

- Enabling this setting will result in this check being done on all symbols (i.e. there will not be an ability to enable on a per symbol basis).

- Check is only available during market hours and will only apply to non-market priced orders in the continuous market.

3.1.8. Fat Finger Protection

**Breach Action:** triggered when calculation > limit. Order rejected on arrival

**Calculation:** incoming order's limit price differs from the NBBO by more than the configured limit

**Configuration:** configurable at the MPID and MPID+Port level

- Reference Price - contra side NBBO. If NBBO is not available, the previous day's Official Closing Price will be used as the reference price. Separate limits can be set depending on the reference price ranges below.

<table>
<thead>
<tr>
<th>RiskRangeID</th>
<th>Reference Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Below $1.00</td>
</tr>
<tr>
<td>2</td>
<td>Equal to $1.00 and Below $10.00</td>
</tr>
<tr>
<td>3</td>
<td>Equal to $10.00 and Below $50.00</td>
</tr>
<tr>
<td>4</td>
<td>Equal to $50.00 and Below $100.00</td>
</tr>
<tr>
<td>5</td>
<td>Equal to $100.00 and Below $500.00</td>
</tr>
<tr>
<td>6</td>
<td>Equal to $500.00 and Above</td>
</tr>
</tbody>
</table>

- **Percentage:** Min: 0% , Max: 500%

- **Notional:** Min 0 , Max: Max Long
Design:

- Each individual order that would exceed the configured limit will be rejected.
- Customers will have the ability to configure Fat Finger limits using both percentage-based limits and/or dollar-based limits.
- When both percentage and dollar-based limits are specified, the more conservative limit will be enforced.

3.1.9. Order Rate Thresholds

3.1.9.1. Duplicative Order Protection

Breach Action: triggered when count of duplicative orders > limit.

Calculation: Duplicative orders that have the same side, price, quantity and symbol that have been entered during a configurable amount of time (in seconds, and specified by the customer) for the same MPID.

Configuration: configurable at the MPID+Port level

- Number of orders: Min: 0 Max: Max Long
- Number of seconds: Min: 1 Max: 30

Design: Each individual order that would exceed the configured limit will be rejected. A breach will require customers to send a Safety Switch command to allow new orders to be entered via the affected port(s).
3.1.9.2. Message Rate Thresholds

Breach Action: triggered when count of messages (Port or Symbol) > limit

Calculation: The maximum number of messages (Port or Symbol) sent in a rolling one second window, calculated from the time a non-heartbeat message is received. All non-cancel messages, via non-dedicated cancel ports, will count towards this threshold.

Configuration: configurable at the MPID+Port level

- Number of messages: Min: 0 Max: Long

Design:

- Once breached, all new orders and modifications will be rejected, and cancels will continue to be accepted via the affected MPID/port. Manual intervention from the firm will be required to re-allow new orders and modifications to be entered via the affected MPID/port.
- A breach will require customers to send a Safety Switch command to allow new orders to be entered via the affected port(s).

3.1.10. Gross Exposure - Open, Executed, Notional

Breach Action: triggered when calculation > limit.

Calculation: Gross Open, Executed, and Notional exposure is calculated at an aggregated basis, at EACH separate exchange (Nasdaq, BX, PSX) and for routed orders.

- Gross Open Exposure
  - [sum of booked price * size for all open buy orders] + [sum of booked price * size for all open sell orders]. Orders exposed will be calculated using the resting order's booked price on the book (which may be less aggressive than the order's entered limit price).

- Gross Executed Exposure
  - [sum of size * trade price for all buy orders executed] + [sum of size * trade price for all sell orders executed].

- Gross Notional Exposure
  - Total open and executed order exposure; (buys executed + buys exposed + sells executed + sells exposed)

Configuration: configurable at the MPID, MPID+Port, and MPID+GroupID

- Min: 1 Max: Long
Design:

- Orders received after the breach is detected will be rejected
- Port auto-unlock will apply if the amount falls under the configured limit.
- For each of the Gross Exposure risk controls, the following options are available as automatic actions if the specific risk control is breached on each individual exchange. This action will be applied to the specific level where the limits configured were breached
  - Reject new orders
  - Reject new orders and cancel all open orders including Opening and Closing Cross orders
  - Reject new orders and cancel all open orders excluding Opening and Closing Cross orders
- Gross Exposure checks offer three threshold levels:
  - **Watch:** exposures exceeding this value will generate an email alert (when configured)
  - **Warn:** exposures exceeding this value will generate an email alert (when configured)
  - **Action:** exposures exceeding this value will generate an email alert (when configured) and trigger the selected Breach Action (Reject, Cancel All, Cancel Non Cross)
3.2. Deleting a rule

- To delete a current rule, select the rule by checking the box to the left and click “Delete”.
- Rule deletions will take immediate effect intraday and the applicable risk settings will no longer be active.
- Rule deletions are not retroactive and will not impact orders entered prior to the deletion.

3.3. View/Edit current rules

- Clicking on each rule tab will display all current risk settings in the table below.
- Rules with a status of ACTIVE are currently being enforced in the trading system.
- Rules with a status of CONFIGURED have been setup but are not yet active. Such rules will automatically become ACTIVE for the next trading session.
• To edit an existing rule, select the rule and click “Edit”.

• When editing CONFIGURED rules, the rules can only be edited using the “Next Day (Configured)” radio button and will take effect when the rule becomes ACTIVE.

• When editing ACTIVE rules, any changes made will take immediate effect and will be applied during the current trading session.

3.4. Audit rules

• Users are able to audit the history of a given rule by selecting the rule and clicking “Audit”.

• User will need to specify the Exchange, MPID, and Date Range

• The audit feature will produce a .CSV file detailing the Revision Date, Revision Type, User, and relevant changes made to the rule.
3.5. Email alerts

- Users are able to create email alerts when breaches occur for any of their established risk settings.
- A user is only allowed to configure email alerts for a MPID, Port, and GroupID to which they have access
- The user need to specify the following when configuring an email alert:
  - Rule Type
  - Exchange
  - MPID/Port/Group ID
  - Email address(es)
- Users can create email alerts directly through the configuration screen for the specific rule or through the Alert Configurations tab:
  - To create an alert through the configuration screen for the specific rule, select the appropriate rule from the EQRC Rules screen and click the “New Alert” button. Select or type the email address that should receive the alerts, check “Configuration Enabled”, and click “Save”.

![Fat Finger Rules](image)
To create an alert through the Alert Configurations tab, navigate to this tab and click on “New”.

- User will have to manually select the applicable risk entities, rule type, and email addresses for the alerts, select “Configuration Enabled”, and click “Save”.

- NOTE: For Gross Exposure checks, an email alert will be received for a breach of each threshold (Watch/Warn/Action).
- Users can view all current email alerts that have been set up through the Alerts Configurations tab in the EQRC Rules menu.
4. Breach and Exposure Monitoring

- The EQRC UI provides users with the ability to monitor risk limit breaches, current exposure levels, as well as the ability to cancel orders/disable ports via the Safety Switch function.
- Users will only be able to see breaches and exposure levels for MPIDs for which they have access.
- When selecting an MPID, users will see all breaches and exposure levels for that MPID and have the ability to further refine the results by Port.

4.1. Breach Monitoring

- The EQRC user interface provides users with the ability to monitor single order and exposure breaches.
- The number of breaches listed for each risk setting represents the cumulative breaches for the MPID or MPID+Port to which the user has access.
4.2. Exposure Monitoring

- The EQRC UI provides users with the ability to monitor current exposure levels against all configured Open Exposure, Executed Exposure, and Notional Exposure rules.
- All active rules will be listed in the “Current Exposure” section of the UI.
- For each established exposure limit, the UI will provide the three threshold levels (Watch, Warn, Action) as well as the current exposure for a given MPID/Port.
- Users can also monitor exposure levels by looking at the threshold bar which displays the level within which the current exposure lies.
- The percentage usage within the current level can be viewed by hovering over the black indicator arrow.

![Current Exposure](image)

4.3. Safety Switch

- The EQRC UI offers users the ability to mass cancel orders (including or excluding cross orders) and/or disable ports via the Safety Switch function.
- Users can perform one or both of these functions in a single command by clicking on the “Actions” button in the EQRC dashboard:
• Users must specify the Exchange, MPID, Port, Cancel Action and/or Port Action for each Safety Switch request.

![Safety Switch interface](image)

• Port disablement requests will only last for the current trading session and will not carry over to the next session
• The Safety Switch is also used to re-enable ports that have been disabled due to prior Safety Switch requests or rate threshold breaches. To re-enable a port, set the Port Action to “Enable” when performing the action.

5. Permissioning and Configurability

5.1. Availability and Permissioning

Availability
• UI will only be available Monday through Friday
• UI will not be available on holidays
• Creation/update/delete will not be allowed EST 8:30pm- 4:30am

Users
• Each user accessing the interface will require a unique user id and password
• Users are permissioned on a service by service level and whether they are allowed read, write, or have other access levels available in the UI.

Roles
1. Read only
   – Allows for reading of rules, breaches, and current exposure in the UI.
2. Read/Write
   – Allows for creation/updating/deletion of rules, reading of breaches and exposure within UI.

5.2. Configurability

Risk Users are firms eligible to set, modify, and view risk check settings. Users also have the ability to analyze the historical usage of the risk checks settings.

*Note: if a specific risk check is configured at multiple hierarchies (e.g. MPID and Group ID) or across both the UI and legacy levels, the most restrictive limit will always be enforced.*
## Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Published</th>
<th>Author(s)</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>30 May 2023</td>
<td>US Equities Product Management</td>
<td>Initial draft</td>
</tr>
</tbody>
</table>