ATOM SOP

The following procedure outlines the steps Fraud Investigations BPO agents should follow when reviewing an account flagged for the ATOM model. The ATOM Login model is designed to detect potential Account Takeover (ATO) when a device logs in. This model provides early detection opportunities to mitigate ATO risks. Accounts with confirmed ATO should go through the Step Up Authorization (SUA) process.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1.</td><td><b>In Unit 21:</b>
<ul><li>Open Unit 21 alert.</li><li>Identify the flagged device (dsml_device_id) and flagged device timestamp (dsml_session_timestamp) from the Custom Data section.</li></ul>Go to the next step.</td></tr>
<tr><td>1a.</td><td><b>In Penny:</b> Check out the email associated with the Chime account. If the domain includes “chime.com” then this is a Chime employee email.

Is the email address domain associated with Chime?
<table>
<tr><th>If</th><th>Then</th></tr>
<tr><td>The email is a Chime employee email.</td><td>Go to step 18.</td></tr>
<tr><td>The email is not a Chime employee email.</td><td>Go to the next step.</td></tr>
</table></td></tr>
<tr><td>1b.</td><td><b>In Penny:</b> Look at the Enrollment Date on the account.
<ul><li>Enter Member ID into the search bar</li><li>Click Search</li><li>Open the member profile</li><li>Click into the <b>Details</b> tab</li><li>Find the <b>Enrolled at</b> date</li></ul>Is the dsml_session_timestamp less than 30 days from the enrollment date?
<table>
<tr><th>If</th><th>Then</th></tr>
<tr><td>The dsml_session_timestamp is less than 30 days from the enrollment date</td><td>Go to step 16.</td></tr>
<tr><td>The dsml_session_timestamp is more</td><td>Go to the next step.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>than 30 days from the enrollment date</td><td></td></tr></table></td></tr>
<tr><td>2.</td><td>

In Penny: You need to locate the flagged device ID along with the flagged timestamp.

- Navigate to Risk Events
- Using the *Search* bar, enter the dsml_device_id and hit Enter

Are you able to locate the flagged Device ID (dsml_device_id) and flagged timestamp (dsml_session_timestamp) in the Risk Events Timeline section of Penny?

<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>Go to the next step.</td></tr><tr><td>No</td><td>Go to step 12.</td></tr></table>

</td></tr>
<tr><td>3.</td><td>

(New device)

Using **Risk Events Timeline (Penny)** OR the **BPO Dashboard (Looker)**:
Was the device first seen within 48 hours of the flagged event?

<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>Go to step 4.</td></tr><tr><td>No</td><td>Go to the next step.</td></tr></table>

</td></tr>
<tr><td>3a.</td><td>

(Established device)

Was the device first seen after account enrollment but more than 48 hours before the flagged event?

<table><tr><th>If</th><th>Then</th></tr><tr><td>Yes</td><td>Go to step 4.</td></tr><tr><td>No</td><td>Go to the next step.</td></tr></table>

</td></tr>
<tr><td>3b.</td><td>

(Historical device)

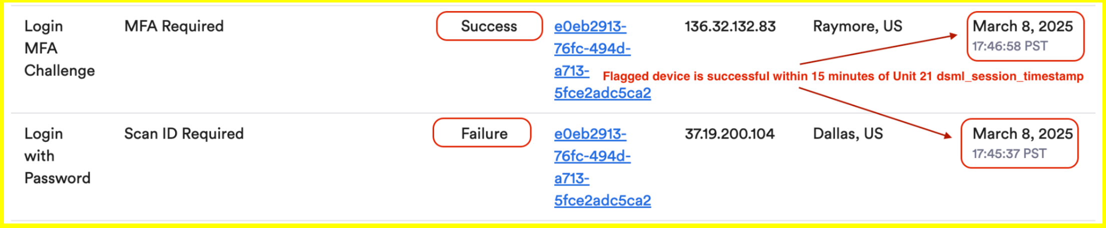
Was the device first seen **on or very near the account enrollment date**?

</td></tr>
</table>

If	Then
Yes	Go to step 16.
No	Go to step 3.

4\.

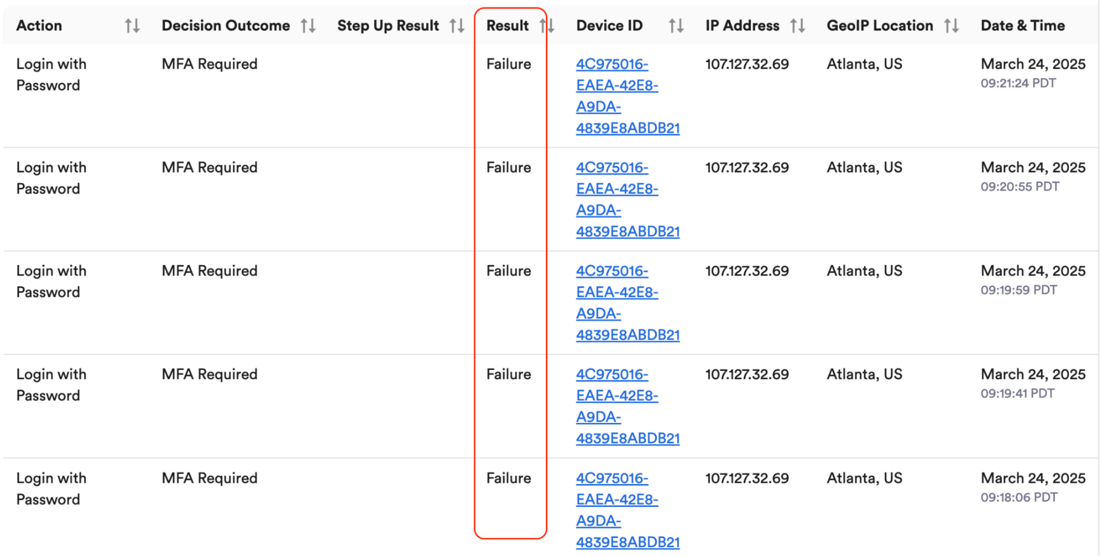
Next, you need to determine if the device was able to successfully login to the Chime account.



Login MFA Challenge	MFA Required	Success	e0eb2913-76fc-494d-a713-5fce2adc5ca2	136.32.132.83	Raymore, US	March 8, 2025 17:46:58 PST
Login with Password	Scan ID Required	Failure	e0eb2913-76fc-494d-a713-5fce2adc5ca2	37.19.200.104	Dallas, US	March 8, 2025 17:45:37 PST

Flagged device is successful within 15 minutes of Unit 21 dsml_session_timestamp

In the screenshot above, the flagged device failed ScanID, but then was able to successfully login a few seconds later by passing the MFA Challenge. This would be a successful device login.



Action	Decision Outcome	Step Up Result	Result	Device ID	IP Address	GeoIP Location	Date & Time
Login with Password	MFA Required		Failure	4C975016-EAEA-42E8-A9DA-4839E8ABDB21	107.127.32.69	Atlanta, US	March 24, 2025 09:21:24 PDT
Login with Password	MFA Required		Failure	4C975016-EAEA-42E8-A9DA-4839E8ABDB21	107.127.32.69	Atlanta, US	March 24, 2025 09:20:55 PDT
Login with Password	MFA Required		Failure	4C975016-EAEA-42E8-A9DA-4839E8ABDB21	107.127.32.69	Atlanta, US	March 24, 2025 09:19:59 PDT
Login with Password	MFA Required		Failure	4C975016-EAEA-42E8-A9DA-4839E8ABDB21	107.127.32.69	Atlanta, US	March 24, 2025 09:19:41 PDT
Login with Password	MFA Required		Failure	4C975016-EAEA-42E8-A9DA-4839E8ABDB21	107.127.32.69	Atlanta, US	March 24, 2025 09:18:06 PDT

In the screenshot above, the flagged device failed every login attempt. This would be a failed login.

Was the flagged device able to successfully login within 15 minutes of the flagged timestamp?

🟤 **SOP Adherence Checkpoint (Flagged Device Login Status):** Was the flagged device able to successfully login to the account? (Yes/No) If yes, insert the timestamp of the successful login if it differs from the flagged timestamp.

If	Then
Failure	Go to step 6 (attempted ATO flow)

Success	Go to the next step.
No Result	Go to step 16.

5. Now you need to look to see what kind of successful login was done.

One Time Passcode: The owner of the device gets a temporary code sent to their phone. They enter this code to log in.
Scan ID: The device owner shows a photo ID (like a driver’s license or passport) and takes a selfie to prove who they are.
Biometric: The owner of the device uses their phone's security features, like fingerprint or face scan. This helps them unlock their phone or log in to the Chime app without typing a password.
Password: The owner of the device used a password to login.
Post-Enrollment Automatic Login: This login happens right after a member first creates an account.
Password with MFA Challenge: The member attempted to login with their password, however it was incorrect. Chime gave the member an option to login via MagicLink and OTP.

What kind of successful login was it?

If	**Then**
OTP	Go to step 8.
Scan ID	Go to step 16
Biometric	Go to step 16.
Password Login	Go to step 8.
Post-Enrollment Automatic Login	Go to step 16.
Password with MFA Challenge	Go to step 8.

6. [Attempted ATO IP Check]

Using **Risk Events Timeline (Penny)** OR the **BPO Dashboard (Looker)**: Look for any of the following red flags about the flagged device IP address:

- Being outside the U.S.
- Being from a state that doesn’t match the member’s current or previous address on file
- Being from a state where the member does not have prior device IP activity

— check carefully for past IPs in that state within the last 6 months

- Device Location does not match any of the member’s physical card transaction locations within the past 6 months

🔵 **SOP Adherence Checkpoint (Flagged Device (CARRIER-1PARTIAL1)):** What red flags/suspicious signals were found in relation to the flagged device(If applicable)?

Were any of the above **true** about the flagged device?

If	**Then**
Yes	Go to step 17.
No	Go to the next step.

7\.

[Attempted ATO Timezone Check]

Using **Risk Events Timeline (Penny)** OR the **BPO Dashboard (Looker)**: Look for any of the following red flags about the flagged device timezone:

- Timezone is associated with an international location
- Timezone is associated with fraudulent activity
  - Common Suspicious Timezones:
    - Africa/Lagos
    - Africa/ Accra
    - Asia/Dubai
    - Asia/Jakarta
    - Asia/Sangai
    - Asia/Karachi
    - Asia/ Dhaka
    - Asia/ HO_CHI_MINH
    - Asia/Kolkata
    - Australia /Perth
    - Asia/ Kathmandu
    - Europe/ London
    - America/Shiprock

🔵 **SOP Adherence Checkpoint (Flagged Device (CARRIER-1PARTIAL1)):** What red flags/suspicious signals were found in relation to the flagged device(If applicable)?

Were any of the above **true** about the flagged device?

If	**Then**
Yes	Go to Step 17.
No	Go to the next step.

<table>
<tr><td></td><td></td></tr>
<tr><td>7a.</td><td>[Attempted ATO Linked Device Check]

Using <b>Risk Events Timeline (Penny)</b> OR the <b>BPO Dashboard (Looker)</b>: Look to see if there are multiple users associated with the flagged device.

Are there multiple other users associated with the flagged device?

🟤 <b>SOP Adherence Checkpoint (Flagged Device Linked Accounts):</b> Is the flagged device linked to other accounts? (Yes/No). If yes, notate whether the linked accounts are suspicious and provide details/signals to support the decision.

<table>
<tr><th>If</th><th>Then</th></tr>
<tr><td>Yes</td><td>Go to the next step</td></tr>
<tr><td>No</td><td>Go to step 16.</td></tr>
</table>
</td></tr>
<tr><td>7b.</td><td>[Attempted ATO Linked Device Check]

Open up the linked users in <b>Penny</b> to look to see if any are linked to the member you are investigating. Linked members would <b>not</b> appear suspicious if they:

<ul>
<li>Currently live or previously lived at the same address as the member</li>
<li>Share the same last name as the member</li>
<li>Are linked to more than one of the member’s devices</li>
<li>Have a previous undisputed p2p transaction with the member</li>
</ul>
🟤 <b>SOP Adherence Checkpoint (Flagged Device Linked Accounts):</b> Is the flagged device linked to other accounts? (Yes/No). If yes, notate whether the linked accounts are suspicious and provide details/signals to support the decision.

Do any members linked to the flagged device meet the above criteria?

<table>
<tr><th>If</th><th>Then</th></tr>
<tr><td>Yes</td><td>Go to step 16.</td></tr>
<tr><td>No</td><td>Go to step 13.</td></tr>
</table>
</td></tr>
<tr><td>8.</td><td>Using <b>Risk Events Timeline (Penny)</b> OR the <b>BPO Dashboard (Looker)</b>: Look for any of the following red flags about the flagged device IP address:</td></tr>
</table>

- Being outside the U.S.
- Being from a state that doesn't match the member's current or previous address on file
- Being from a state where the member does not have prior device IP activity — check carefully for past IPs in that state within the last 6 months
- Device Location does not match any of the member's physical card transaction locations within the past 6 months

🔵 **SOP Adherence Checkpoint (Flagged Device (CARRIER-1PARTIAL1)):** What red flags/suspicious signals were found in relation to the flagged device(If applicable)?

Were any of the above **true** about the flagged device?

If	**Then**
Yes	Go to step 13.
No	Go to the next step.

9. Using **Risk Events Timeline (Penny)** OR the **BPO Dashboard (Looker)**: Look for any of the following red flags about the flagged device timezone:

- Timezone is associated with an international location
- Timezone is associated with fraudulent activity
    - Common Suspicious Foreign Time Zones:
        - Africa/Lagos
        - Africa/ Accra
        - Asia/Dubai
        - Asia/Jakarta
        - Asia/Sangai
        - Asia/Karachi
        - Asia/ Dhaka
        - Asia/ HO_CHI_MINH
        - Asia/Kolkata
        - Australia /Perth
        - Asia/ Kathmandu
        - Europe/ London
        - America/Shiprock

🔵 **SOP Adherence Checkpoint (Flagged Device (CARRIER-1PARTIAL1)):** What red flags/suspicious signals were found in relation to the flagged device(If applicable)?

Were any of the above **true** about the flagged device?

If	**Then**

<table>
<tr><td></td><td>
<table>
<tr><td>Yes</td><td>Go to step 13.</td></tr>
<tr><td>No or N/A</td><td>Go to the next step.</td></tr>
</table>
</td></tr>
<tr><td>10.</td><td>
Using **Risk Events Timeline (Penny)** OR the **BPO Dashboard (Looker)**: Look to see if there are multiple users associated with the flagged device.

Are there multiple other users associated with the flagged device?

🟤 **SOP Adherence Checkpoint (Flagged Device Linked Accounts):** Is the flagged device linked to other accounts? (Yes/No). If yes, notate whether the linked accounts are suspicious and provide details/signals to support the decision.

<table>
<tr><th>If</th><th>Then</th></tr>
<tr><td>Yes</td><td>Go to the next step.</td></tr>
<tr><td>No</td><td>Go to step 16.</td></tr>
</table>
</td></tr>
<tr><td>11.</td><td>
Open up the linked users in **Penny** to look to see if any are linked to the member you are investigating. Linked members would **not** appear suspicious if they:

- Currently live or previously lived at the same address as the member
- Share the same last name as the member
- Are linked to more than one of the member’s devices
- Have a previous undisputed p2p transaction with the member

🟤 **SOP Adherence Checkpoint (Flagged Device Linked Accounts):** Is the flagged device linked to other accounts? (Yes/No). If yes, notate whether the linked accounts are suspicious and provide details/signals to support the decision.

Do any members linked to the flagged device meet the above criteria?

<table>
<tr><th>If</th><th>Then</th></tr>
<tr><td>Yes</td><td>Go to step 16.</td></tr>
<tr><td>No</td><td>Go to step 13.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>12.</td><td><b>In Looker:</b> Search the Member ID and locate the flagged device ID in either the <b>Device Linkage</b> section, the <b>Amplitude Events</b> section or the <b>ATO Login</b> section.

Are you able to locate the flagged Device ID (dsml_device_id) and flagged timestamp (dsml_session_timestamp) from the Unit 21 Custom Data section?

<table>
<tr><th>If</th><th>Then</th></tr>
<tr><td>Yes</td><td>Go to step 3.</td></tr>
<tr><td>No</td><td>Go to step 16.</td></tr>
</table></td></tr>
<tr><td>13.</td><td><b>In Penny:</b> Navigate to the member’s Penny profile > Details > History tab to look for PI changes within 24 hours of the flagged device login.

Are there PI changes within 24 hours of the flagged device login?

🟠 <b>SOP Adherence Checkpoint (Account Updates):</b> Notate any relevant PI Changes (if applicable) - What changes were made? What device made the change? Why is the change(s) suspicious or not?

<table>
<tr><th>If</th><th>Then</th></tr>
<tr><td>Yes</td><td>Go to the next step.</td></tr>
<tr><td>No</td><td>Go to step 14a.</td></tr>
</table></td></tr>
<tr><td>14</td><td><b>Using Looker or Risk Events Timeline:</b> Determine what device made the PI changes.

🟠 <b>SOP Adherence Checkpoint (Account Updates):</b> Notate any relevant PI Changes (if applicable) - What changes were made? What device made the change? Why is the change(s) suspicious or not?

What device made the PI changes?

Go to the next step.</td></tr>
<tr><td>14a.</td><td>Navigate to the member’s Zendesk page.

Is there any recent outreach from the member with ATO language regarding:
<ul>
<li>Unauthorized PI changes</li>
<li>Unauthorized transactions or the need to file a dispute</li>
<li>Member giving their login credentials to a Chime impersonator</li>
<li>Member claiming they won a Chime sweepstakes and they let someone into</li>
</ul></td></tr>
</table>

<table>
<tr>
<td></td>
<td>their account
● Member was kicked out of account/unable to login with their password
● Unauthorized device is accessing the account

🟢 <b>SOP Adherence Checkpoint (Zendesk Activity):</b> Call out any member outreach regarding ATO in Zendesk (if applicable) - include the ZD Ticket # and a brief summary of the member communication

Go to step 15.</td>
</tr>
<tr>
<td>15</td>
<td>True Positive (<b>ATO</b>) Steps:

Proceed based on the following:

<table>
<tr><th>If</th><th>Then</th></tr>
<tr>
<td>The account is not in Step Up Auth.</td>
<td>● In Penny:
○ Trigger Step Up Auth.
○ Leave Account Notation: <i>//ML_Model//RISK-FC//DSML_ATOMv3_Login</i>
● In Zendesk:
○ Send Zendesk Outreach: Use the ATOM Login Macro “ATOM Login > subtitle is FraudOps Investigations::Info::Suspected ATO::Step Up Auth Victim (Outreach)”
■ Submit as Pending
● In GSheets:
○ Add unusual device to the Genpact Device Block List Prep.
● In Unit 21:
○ Submit your narrative
○ Select True Positive Workflow
○ Select ATO label
○ Close case.</td>
</tr>
<tr>
<td>The account has already been actioned and has Step Up Auth triggered, is suspended or is closed.</td>
<td>● In Penny:
○ Leave Account Notation: <i>//ML_Model//RISK-FC//DSML_ATOMv3_Login_no_action</i>
● In Gsheets:
○ Add unusual device to</td>
</tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td><table><tr><td></td><td>the Genpact Device Block List Prep.
● In Unit 21:
○ Submit your narrative
○ Select True Positive Workflow
○ Select ATO label: unauthorized_account_access_ato
○ Close case.</td></tr></table></td></tr>
<tr><td>16.</td><td>False Positive Steps:
● In Penny:
○ Leave Account Notation: <i>//ML_Model//RISK-FC//DSML_ATOMv3_Login_no_action</i>
● In Unit 21:
○ Submit your narrative
○ Select False Positive Workflow
○ Select Not ATO label: authorized_account_access
○ Submit case.</td></tr>
<tr><td>17.</td><td>True Positive (<b>Password Compromised</b>) Steps:

Proceed based on the following:
<table><tr><td>The account is not in Step Up Auth.</td><td>● In Penny:
○ Trigger Step Up Auth.
○ Leave Account Notation: <i>//ML_Model//RISK-FC//DSML_ATOMv3_Login</i>
● In Zendesk:
○ Send Zendesk Outreach: Use the ATOM Login Macro “ATOM Login > subtitle is FraudOps Investigations::Info::Suspected ATO::Step Up Auth Victim (Outreach)”
■ Submit as Pending
● In GSheets:
○ Add unusual device to the Genpact Device Block List Prep.
● In Unit 21:
○ Submit your narrative</td></tr></table></td></tr>
</table>

		○ Select True Positive Workflow ○ Select Password Compromised label: unauthorized_account_access_password_compromised ○ Close case.
	The account has already been actioned and has SUA triggered, is suspended or is closed.	● In Penny: ○ Leave Account Notation: *//ML_Model//RISK-FC//DSML_ATOMv3_Login_no_action* ● In Gsheets: ○ Add unusual device to the Genpact Device Block List Prep. ● In Unit 21: ○ Submit your narrative ○ Select True Positive Workflow ○ Select Password Compromised label: unauthorized_account_access_password_compromised ○ Close case.
18.	Chime employee account: ● In Unit 21: Assign this alert to Lizzy Powers ● Let your lead know that you were assigned an alert for an account belonging to a Chime employee.	

SOP Adherence Checkpoint Steps:

🛑 **SOP Adherence Checkpoint (Flagged Device (CARRIER-1PARTIAL1)):** What red flags/suspicious signals were found in relation to the flagged device(If applicable)?
🛑 **SOP Adherence Checkpoint (Flagged Device Linked Accounts):** Is the flagged device linked to other accounts? (Yes/No). If yes, notate whether the linked accounts are suspicious and provide details/signals to support the decision.
🛑 **SOP Adherence Checkpoint (Flagged Device Login Status):** Was the flagged device able to successfully login to the account? (Yes/No) If yes, insert the timestamp of the successful login if it differs from the flagged timestamp.

🛑 **SOP Adherence Checkpoint (Zendesk Activity):** Call out any member outreach regarding ATO in Zendesk (if applicable) - include the ZD Ticket # and a brief summary of the member communication
🛑 **SOP Adherence Checkpoint (Account Updates):** Notate any relevant PI Changes (if applicable) - What changes were made? What device made the change? Why is the change(s) suspicious or not?

Reference:
Attempted ATO True Positive case: https://chime.unit21.com/alerts/4701962/custom-data
False Positive case:
True Positive ATO: https://chime.unit21.com/alerts/4700133/prior-activity

Testing Sheet: ATOM Decision Tree Test Sheet