SmartApps

Reports Guide v1.0

CX Optimized

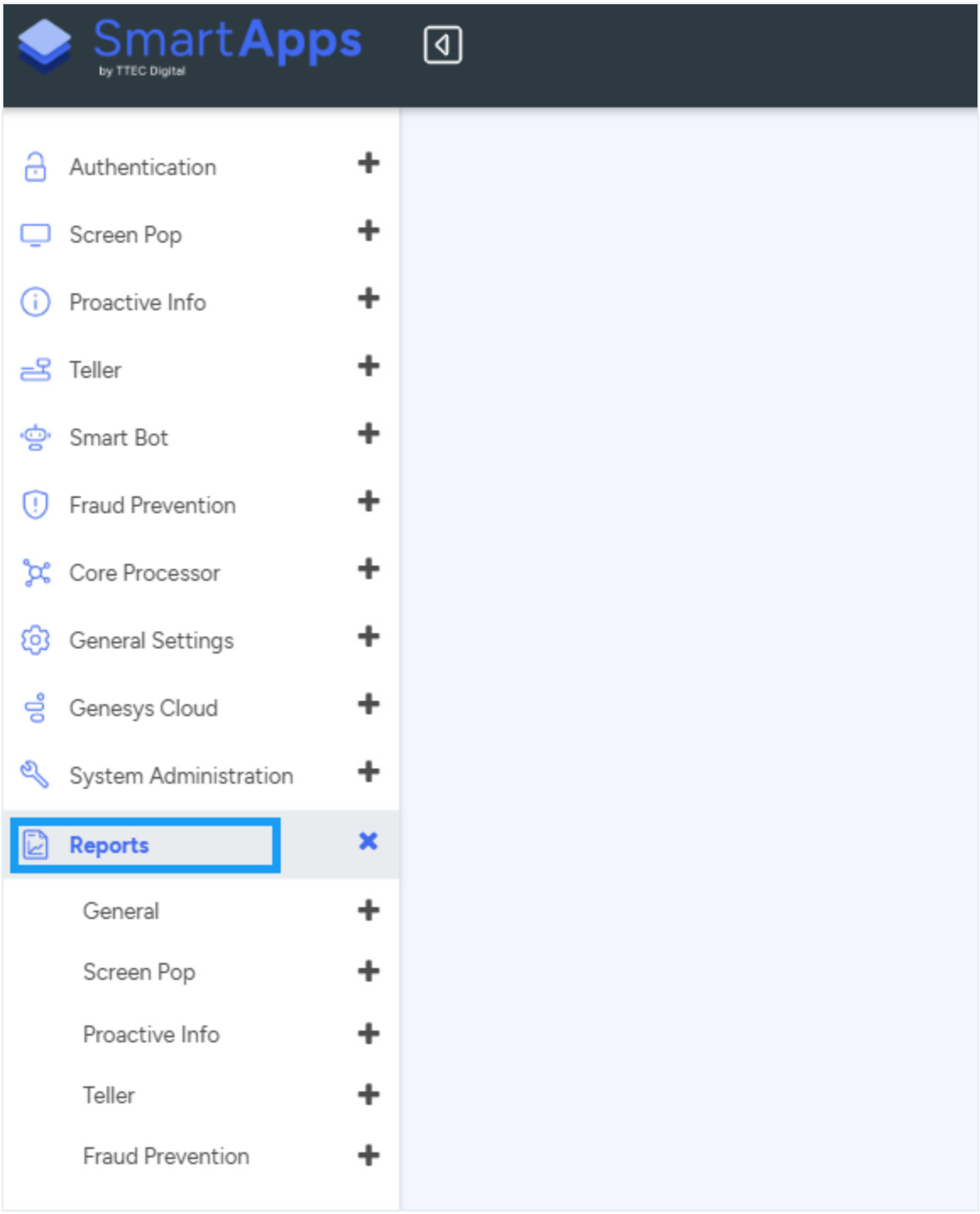
Table of Contents

Reports

The Reports section provides comprehensive instructions on how to effectively use the reporting features of SmartApps.

How to access and generate reports

1. **Log in**: to **SmartApps Site Manager** using your credentials (email-address, password).
2. **Navigate**: to the **Reports** section from the left-side navigation pain in the main dashboard.
3. **Select Report**: Choose the required report.
4. **Define Parameters**: Set the time-period, member segments, or other criteria.
5. **Generate Report**: Click, **Run Report** to generate the report.
6. **Review and Save**: Review the generated report for accuracy and save it as needed.


SmartApps
by TTEC Digital
Authentication
Screen Pop
Proactive Info
Teller
Smart Bot
Fraud Prevention
Core Processor
General Settings
Genesys Cloud
System Administration
Reports
General
Screen Pop
Proactive Info
Teller
Fraud Prevention

Account Types

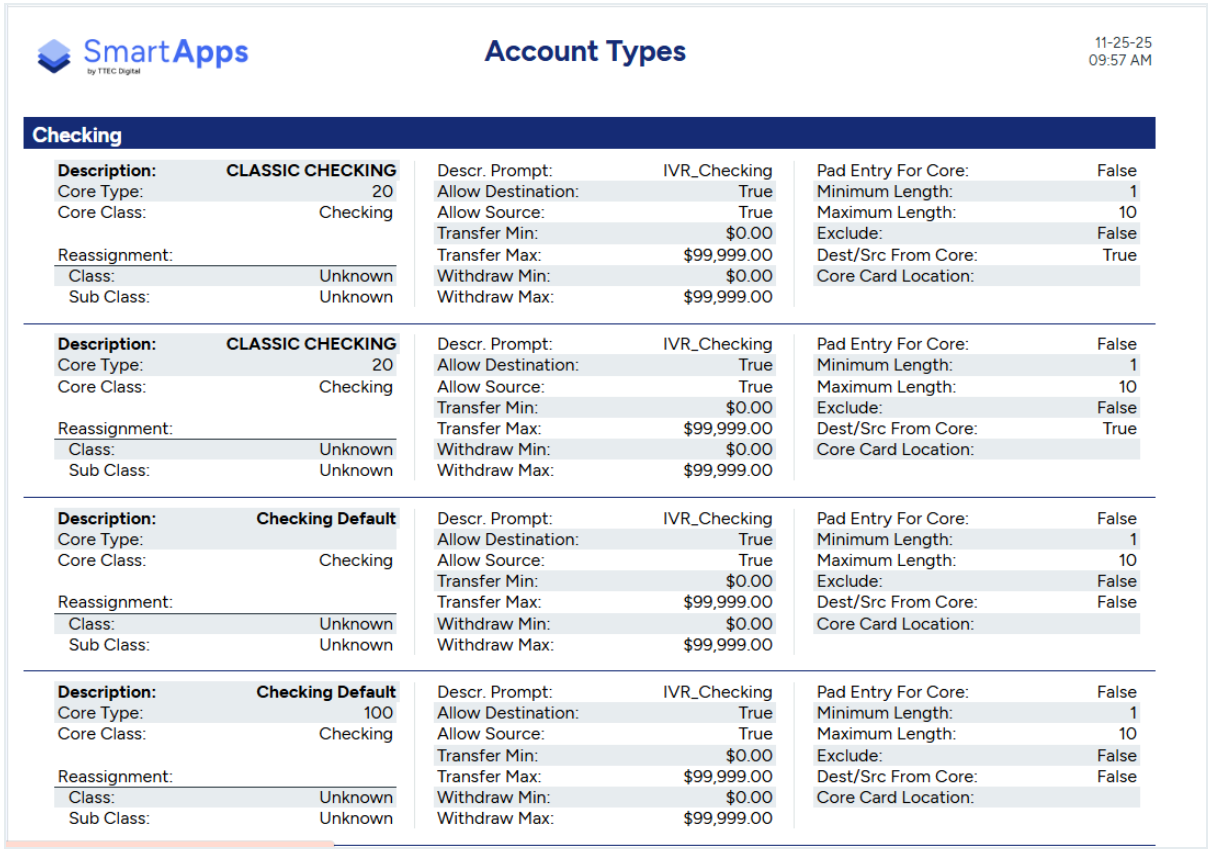
Description

This report defines **account type configurations** used by SmartApps, including parameters such as **transaction limits**, **core system mappings**, and **permissions** for transfers, withdrawals, and deposits.

These configurations ensure that each account type — such as Checking, Savings, Loans, IRAs, Certificates of Deposit, Mortgages or Credit Cards — behaves correctly across digital banking and IVR channels.

SmartApps uses this setup to determine:

- Which accounts can be used for **transfers**, **withdrawals**, or **deposits**
- How each account is **identified in the core system**
- Which accounts are eligible as **transfer sources or destinations**
- The correct **IVR prompts and labels** that will play to members or display on the screens
- Whether an account is **visible or excluded** from member-facing systems



SmartApps by TTEC Digital

Account Types

11-25-25
09:57 AM

Checking

Description:	**CLASSIC CHECKING**	Descr. Prompt:	IVR_Checking	Pad Entry For Core:	False
Core Type:	20	Allow Destination:	True	Minimum Length:	1
Core Class:	Checking	Allow Source:	True	Maximum Length:	10
		Transfer Min:	$0.00	Exclude:	False
Reassignment:		Transfer Max:	$99,999.00	Dest/Src From Core:	True
Class:	Unknown	Withdraw Min:	$0.00	Core Card Location:	
Sub Class:	Unknown	Withdraw Max:	$99,999.00		

Description:	**CLASSIC CHECKING**	Descr. Prompt:	IVR_Checking	Pad Entry For Core:	False
Core Type:	20	Allow Destination:	True	Minimum Length:	1
Core Class:	Checking	Allow Source:	True	Maximum Length:	10
		Transfer Min:	$0.00	Exclude:	False
Reassignment:		Transfer Max:	$99,999.00	Dest/Src From Core:	True
Class:	Unknown	Withdraw Min:	$0.00	Core Card Location:	
Sub Class:	Unknown	Withdraw Max:	$99,999.00		

Description:	**Checking Default**	Descr. Prompt:	IVR_Checking	Pad Entry For Core:	False
Core Type:		Allow Destination:	True	Minimum Length:	1
Core Class:	Checking	Allow Source:	True	Maximum Length:	10
		Transfer Min:	$0.00	Exclude:	False
Reassignment:		Transfer Max:	$99,999.00	Dest/Src From Core:	False
Class:	Unknown	Withdraw Min:	$0.00	Core Card Location:	
Sub Class:	Unknown	Withdraw Max:	$99,999.00		

Description:	**Checking Default**	Descr. Prompt:	IVR_Checking	Pad Entry For Core:	False
Core Type:	100	Allow Destination:	True	Minimum Length:	1
Core Class:	Checking	Allow Source:	True	Maximum Length:	10
		Transfer Min:	$0.00	Exclude:	False
Reassignment:		Transfer Max:	$99,999.00	Dest/Src From Core:	False
Class:	Unknown	Withdraw Min:	$0.00	Core Card Location:	
Sub Class:	Unknown	Withdraw Max:	$99,999.00		

Key Concepts

- **Core Mapping**

  SmartApps integrates directly with your core banking system, using **Core Type** and **Core Class** codes to identify account types. These codes determine how account and product data are interpreted within SmartApps.

  In instances where the core system utilizes generic, inconsistent, or overly broad classifications, SmartApps provides a **Reassignment** field. This feature allows administrators to redefine or further specify how a product should be displayed and treated within SmartApps.

> **Notes:**
>
> **Account Type Reclassification**: The core system may classify an account as a Savings account. ***Reassignment*** allows SmartApps to correctly identify and process the account as an IRA, ensuring the product is handled according to its actual purpose.
>
> **Loan Product Differentiation**: The core may designate a product simply as a Loan. Within SmartApps, ***Reassignment*** allows this product to be defined as either an Open-End Loan or a Closed-End Loan. This differentiation determines the system functionality, available features, and treatment rules that apply to the loan product.

- **Transaction Permissions**

  Each account type specifies whether it can act as a **source** (send funds), **destination** (receive funds), or both.

  - Checking and Savings accounts usually allow both.
  - IRAs and Certificates of Deposit typically allow destination only transfers.
  - Loans often allow payments in (destination), but not out (source).

- **Prompt Integration**

  Every account type links to a Description Prompt (e.g., IVR_Checking, IVR_Loan) that controls what is played to the caller in the automated phone and voice systems.

- **Exclusions**

  Certain account types may exist in the core but are flagged as **Excluded** in SmartApps. These are not shown to members in online banking or IVR — for example, **internal testing accounts**, **charge-offs**, or **overdraft lines**.

- **Padding Rules**

Some core systems require account numbers of fixed length. The **Pad Entry For Core** field indicates if account numbers should be padded with zeros to meet the length requirement.

- **Transaction Limits**

  Each account type includes **Transfer** and **Withdrawal** minimums and maximums. These define allowed transaction ranges and are critical for fraud prevention and compliance.

- **Core Card Location**

  Used for **credit cards or special internal accounts**, this indicates where the card data is managed — typically Internal or blank if not applicable.

What you will see in the report

Field	Description
Description	Account name as displayed to users (e.g., "Classic Checking", "72 Month Auto Loan").
Descr. Prompt	Name of the prompt which will be played to caller for a description of the account type)e.g., IVR_Checking, IVR_Savings.
Core Type/Core Class	The combination of Core Type and Core Class which define an Account Type.
Reassignment Class Sub Class	Allows SmartApps to reclassify or rename accounts to match the institutions desired business rules/-functionality.
Allow Source / Destination	Indicates how the account can be used in Funds Transfer. Allow Source: account can be used to send funds. Allow Destination: account can be used to receive funds.

Field	Description
Transfer / Withdraw Limits	Minimum and maximum transaction amounts allowed for transfers or withdrawals.
Minimum / Maximum Length	The valid account number length for that account type (e.g., 10 digits for checking, 16 for credit cards).
Pad Entry For Core	Specifies if account numbers should be zero-padded before submission to the core system.
Dest./ Source From Core	Determines whether permissions (send/ receive) are inherited directly from the core configuration.
Exclude	Flags accounts that should not appear in IVR or member-facing systems
Core Card Location	Indicates where card data processing occurs within a Symitar system. The card can be handled internally or externally. This field will always be Internal for all other cores.

Application

Use this report to:

- **Audit** account setup and verify configuration accuracy.
- **Validate** transaction permissions(source/ destination rules).
- **Troubleshoot** member-facing issues in IVR, online banking, or mobile apps.
- **Confirm** that SmartApps classifications align with your core system.

> **Example:** A credit union notices members cannot transfer funds from their IRA accounts. The report shows that IRA types have Allow Source = 'False' and Allow Destination = 'True', confirming the system is behaving as designed.

Tips for Users

- Run this report **after system updates** or **during on-boarding** to confirm account mapping is correct.
- Review it when **members report transfer or visibility issues**.
- Share it with business analysts, auditors, and compliance teams to **validate product configuration**.
- Use the **Reassignment** and **Exclude** fields to ensure member-facing names are clear and appropriate.

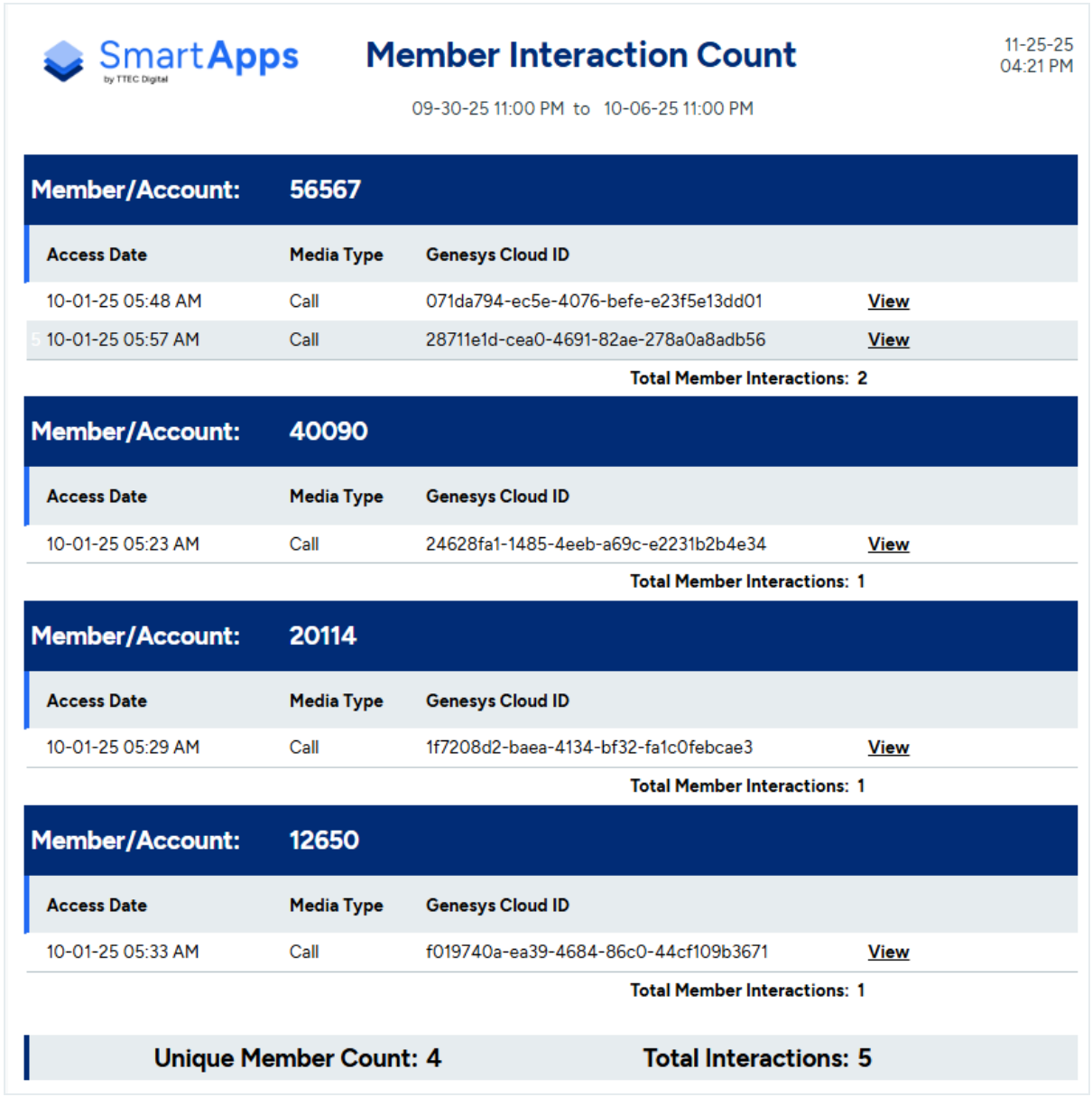
Member Interaction Count

Description

The Member Interaction Count Report provides a detailed summary of how members engage with your financial institution across different communication channels — including **calls**, **emails**, and **chats** — within a defined time period.

This report helps institutions:

- Measure **member engagement** and interaction volume
- Identify **high-contact members** or accounts that may require follow-up
- Investigate **unusual or potentially fraudulent activity**
- Assess **channel performance** for service delivery improvements



SmartApps by TTEC Digital

Member Interaction Count

11-25-25
04:21 PM

09-30-25 11:00 PM to 10-06-25 11:00 PM

Member/Account: 56567

Access Date	Media Type	Genesys Cloud ID	
10-01-25 05:48 AM	Call	071da794-ec5e-4076-befe-e23f5e13dd01	View
10-01-25 05:57 AM	Call	28711e1d-cea0-4691-82ae-278a0a8adb56	View

Total Member Interactions: 2

Member/Account: 40090

Access Date	Media Type	Genesys Cloud ID	
10-01-25 05:23 AM	Call	24628fa1-1485-4eeb-a69c-e2231b2b4e34	View

Total Member Interactions: 1

Member/Account: 20114

Access Date	Media Type	Genesys Cloud ID	
10-01-25 05:29 AM	Call	1f7208d2-baea-4134-bf32-fa1c0febcae3	View

Total Member Interactions: 1

Member/Account: 12650

Access Date	Media Type	Genesys Cloud ID	
10-01-25 05:33 AM	Call	f019740a-ea39-4684-86c0-44cf109b3671	View

Total Member Interactions: 1

Unique Member Count: 4 **Total Interactions: 5**

Key Concepts

- **Chronological View**

  Interactions are listed in **date and time order**, grouped by **member ID** to provide a clear time-line of events and engagement history.

- **Media Types**

  The report includes all supported **communication channels** (calls, emails, chats) equally, allowing for full visibility into multi-channel member behavior.

- **Scalability**

  For institutions with **large member volumes** or extended date ranges, the report may contain a high number of records. Consider filtering by channel to optimize performance.

What you will see in the report

Field	Description
Member ID	Unique identifier assigned to each member within your core system. Used to correlate interactions across channels.
Interaction Type	Communication method used — typically **Call**, **Email**, or **Chat**.
Date & Time	The exact time-stamp of when the interaction occurred.
Genesys Cloud ID	The unique interaction or conversation ID assigned by Genesys Cloud for system traceability.
Total Interactions	The total number of recorded interactions for the member during the reporting period.
Unique Member Count	The number of distinct members who interacted with your institution during the selected time range.
Print Details Option	Allows inclusion or exclusion of detailed interaction logs when exporting or printing the report.

Application

Use this report to:

- **Track member engagement** across all channels.
- **Audit communication history** for specific members or inquiries.
- **Identify patterns** in member behavior or recurring service issues.
- **Investigate anomalies** such as excessive contact or duplicate requests.

> **Example:** A member reports suspicious activity on their account. You run the report for their Member ID and see 12 interactions over the past week—6 calls, 4 chats, and 2 emails. This helps you verify the time-line and investigate further.

Tips for Users

- Use the **Print Details** toggle to switch between summary and full interaction logs.
- Run the report **weekly or monthly** to track engagement trends.
- **Filter by Interaction Type** to focus on a specific communication channel.
- Combine this report with **Usage Summary** to correlate communication volume with system usage.

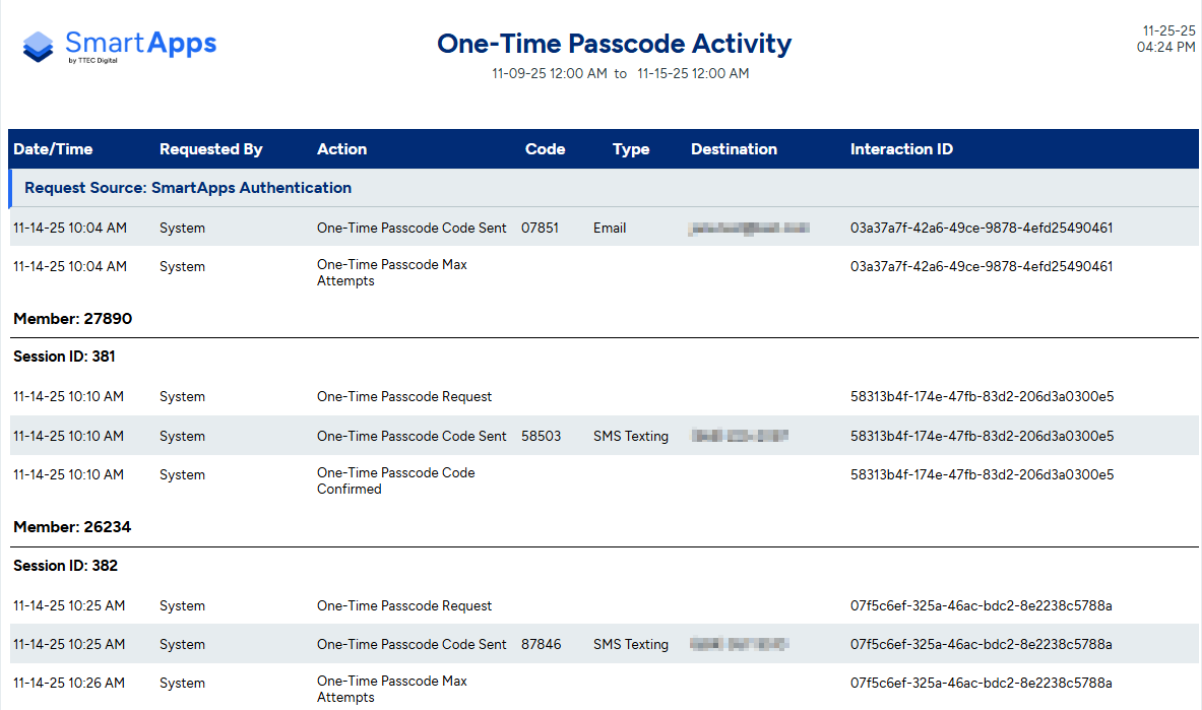
One Time Passcode Activity

Description

The One-Time Passcode (OTP) Activity Report records all authentication events initiated by members or agents that use **temporary verification codes** for identity confirmation.

It captures when a passcode is **requested, sent, confirmed, along with corresponding session identifiers, delivery details, and interaction references.**

This report is essential for monitoring **authentication flow performance**, troubleshooting **access or delivery issues**, and maintaining **security and compliance standards**.



SmartApps by TTEC Digital

One-Time Passcode Activity

11-09-25 12:00 AM to 11-15-25 12:00 AM

11-25-25 04:24 PM

Date/Time	Requested By	Action	Code	Type	Destination	Interaction ID
Request Source: SmartApps Authentication						
11-14-25 10:04 AM	System	One-Time Passcode Code Sent	07851	Email	[redacted]	03a37a7f-42a6-49ce-9878-4efd25490461
11-14-25 10:04 AM	System	One-Time Passcode Max Attempts				03a37a7f-42a6-49ce-9878-4efd25490461
Member: 27890						
Session ID: 381						
11-14-25 10:10 AM	System	One-Time Passcode Request				58313b4f-174e-47fb-83d2-206d3a0300e5
11-14-25 10:10 AM	System	One-Time Passcode Code Sent	58503	SMS Texting	[redacted]	58313b4f-174e-47fb-83d2-206d3a0300e5
11-14-25 10:10 AM	System	One-Time Passcode Code Confirmed				58313b4f-174e-47fb-83d2-206d3a0300e5
Member: 26234						
Session ID: 382						
11-14-25 10:25 AM	System	One-Time Passcode Request				07f5c6ef-325a-46ac-bdc2-8e2238c5788a
11-14-25 10:25 AM	System	One-Time Passcode Code Sent	87846	SMS Texting	[redacted]	07f5c6ef-325a-46ac-bdc2-8e2238c5788a
11-14-25 10:26 AM	System	One-Time Passcode Max Attempts				07f5c6ef-325a-46ac-bdc2-8e2238c5788a

Key Concepts

- **Session Continuity**

  If a member or agent reconnects within the session window, SmartApps recognizes the session and allows them to continue without restarting authentication.

- **Interaction ID Changes**

  When a member confirms a code in a separate call or contact, a new **Interaction ID** may be generated while the **Session ID** remains constant — linking all related OTP attempts within one session.

- **Delivery Tracking**

  Displays the destination channel (e.g., mobile number or email address) where the passcode was sent. This information helps verify that the correct contact method was used and supports troubleshooting when delivery issues occur.

- **Summary Totals**

  At the bottom of the report, SmartApps displays aggregate counts of all OTP messages sent (by SMS and Email) during the selected period. This helps institutions assess overall authentication activity and detect usage trends.

What you will see in the report

Field	Description
Member ID	Identifier of the member associated with the authentication event.
Session ID	A unique identifier for the authentication session that links all related OTP events.
Interaction ID	Identifier for the specific interaction associated with the

Field	Description
	OTP request. Identifies the specific call or digital interaction associated with the code request or confirmation.
Requested By	Indicates whether the request was made by the member or automatically by the system.
Action / Code	Describes the type of OTP event (e.g., One-Time Passcode Request, Confirmation, or Expiration).
Destination	The address or channel where the OTP was sent (e.g., phone number, email).
Date/Time	Date and time when the passcode was generated, sent, and/or confirmed.
Total SMS Messages Sent	Count of SMS-based OTP messages sent during the report period.
Total Email Messages Sent	Count of email-based OTP messages sent during the report period.

Application

Use this report to:

- **Audit** all one-time passcode events for security and compliance validation.
- **Investigate** failed, delayed, or unconfirmed authentication attempts.
- **Verify** delivery channels and ensure contact data accuracy.
- **Analyze** OTP usage trends for system performance monitoring.
- **Support** member service teams when resolving login or access issues.

> **Example:** A member reports not receiving their one-time passcode. Running this report shows the code was sent to an outdated email address. This confirms the issue and allows staff to update the member's contact information.

Tips for Users

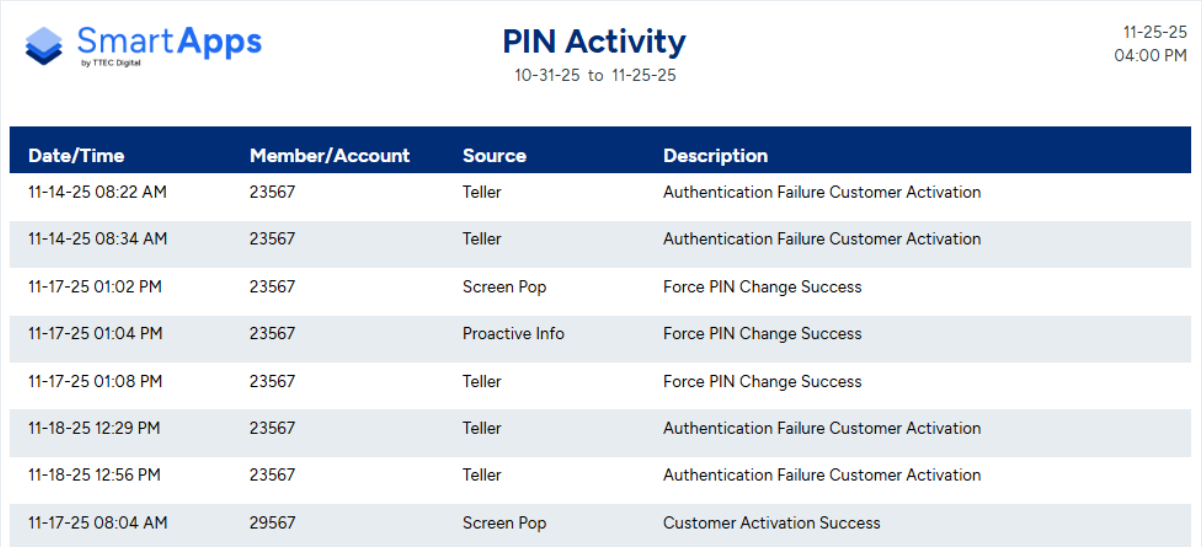
- Use this report to validate **code delivery and confirmation results** during access troubleshooting.
- Run it for **specific member IDs** to resolve login issues or suspicious activity.
- Monitor **session continuity** to understand member retry patterns.
- Review **SMS and Email** totals to track communication volumes.
- Share findings with **security, IT, or compliance teams** for ongoing monitoring and audit purposes.

PIN Activity

Description

The PIN Activity Report captures all activity related to **Personal Identification Numbers** (PINs), including **setup**, **changes**, **resets** and **PIN change authentication attempts**. This report only includes authentication attempts made during a PIN change or customer activation process.

This report supports **security monitoring**, **compliance verification**, and **member access troubleshooting** by providing a full audit trail of PIN-related events.



SmartApps by TTEC Digital

PIN Activity

10-31-25 to 11-25-25

11-25-25
04:00 PM

Date/Time	Member/Account	Source	Description
11-14-25 08:22 AM	23567	Teller	Authentication Failure Customer Activation
11-14-25 08:34 AM	23567	Teller	Authentication Failure Customer Activation
11-17-25 01:02 PM	23567	Screen Pop	Force PIN Change Success
11-17-25 01:04 PM	23567	Proactive Info	Force PIN Change Success
11-17-25 01:08 PM	23567	Teller	Force PIN Change Success
11-18-25 12:29 PM	23567	Teller	Authentication Failure Customer Activation
11-18-25 12:56 PM	23567	Teller	Authentication Failure Customer Activation
11-17-25 08:04 AM	29567	Screen Pop	Customer Activation Success

Key Concepts

- **Customer Activation**

  The initial setup of a first time caller with a new member PIN.

- **PIN Reset / Force PIN Change**

Triggered when security policies require a reset after repeated failed attempts or lockouts.

- **PIN Change Authentication Attempts**

  Authentication attempts made during a PIN change or activation — not general logins.

- **Audit Trail**

  Provides a chronological record of PIN-related activities for review and compliance.

What you will see in the report

Field	Description
Member ID	Identifier for the member performing the PIN-related activity. Optional for broad report runs.
Time-stamp	The exact date and time when the event occurred.
Source	The system or interface where the activity originated (Teller, Screen Pop, Proactive Info, etc.).
Description	The event type and outcome, such as Customer Activation Success, Authentication Failure – Customer Activation, Force PIN Change Failure, or Manual PIN Change Success.

Application

Use this report to:

- Investigate **PIN setup and activation issues** for members.
- Confirm whether authentication attempts were made during **PIN changes or activations**.

- Identify **patterns of repeated PIN change failures** that may indicate user confusion or potential fraudulent activity.
- Validate that **PIN security policies** (like forced changes after failures) are functioning correctly.
- Support member service teams **in explaining lockouts or access issues** clearly.

> **Example:** A member (Account 20890) contacts the credit union after several failed attempts to activate their account. The agent reviews the PIN Activity Report and finds the following sequence of entries:

Date/ Time	Member/ Account	Source	Description
07-02-24 09:13 AM	20890	Teller	Force PIN Change Failure
07-03-24 08:15 AM	20890	Teller	Authentication Failure – Customer Activation
07-03-24 08:23 AM	20890	Teller	Customer Activation Failure
07-03-24 11:08 AM	20890	Teller	Force PIN Change Failure
07-09-24 09:48 AM	20890	Screen Pop	Authentication Failure – Customer Activation
07-09-24 10:00 AM	20890	Teller	Customer Activation Success

Interpretation:

- The member had multiple authentication and activation failures across different days and channels.
- A **forced PIN change** was triggered after repeated failures.
- The final entry shows a **successful customer activation**, confirming the issue was resolved.

Outcome: The agent can confirm that the member's access issue resulted from authentication failures during activation, not a system error, and guide them through proper recovery procedures.

Tips for Users

- Use **Member ID filters** to isolate specific member activity.
- Watch for **repeated Force PIN Change or Authentication Failure events**, as these may indicate risk or confusion.
- Combine this report with the **Fraud Prevention – Member Activity** report for a complete picture of authentication behavior.
- Regularly review **Customer Activation Success** entries to confirm proper on-boarding completion.
- For compliance reviews, export the data to support **security audit documentation.**

Usage Summary

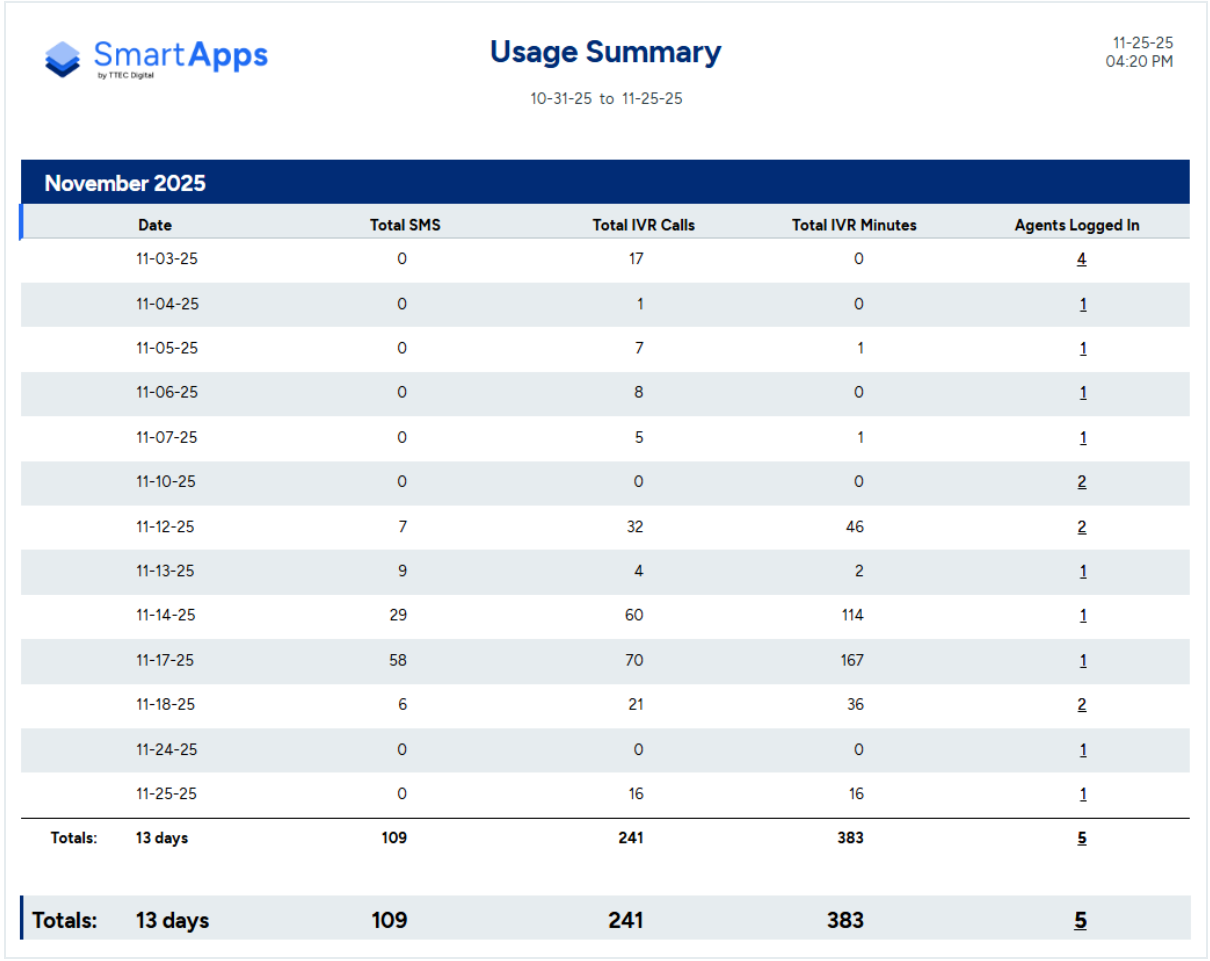
Description

The Usage Summary Report provides a comprehensive overview of your institution's use of **SmartApps communication channels** — specifically **SMS messages**, **IVR (Interactive Voice Response) calls**, and **agent activity** — over a selected time period.

This report helps administrators and managers:

- Monitor **system and channel utilization**
- Track **IVR and SMS consumption** against contractual limits
- Review **agent login activity and workload distribution**
- Prevent **unexpected overage charges** on monthly billing

It serves as a key tool for **usage tracking, operational oversight,** and **billing verification**.



SmartApps by TTEC Digital

Usage Summary

10-31-25 to 11-25-25

11-25-25
04:20 PM

November 2025

Date	Total SMS	Total IVR Calls	Total IVR Minutes	Agents Logged In
11-03-25	0	17	0	4
11-04-25	0	1	0	1
11-05-25	0	7	1	1
11-06-25	0	8	0	1
11-07-25	0	5	1	1
11-10-25	0	0	0	2
11-12-25	7	32	46	2
11-13-25	9	4	2	1
11-14-25	29	60	114	1
11-17-25	58	70	167	1
11-18-25	6	21	36	2
11-24-25	0	0	0	1
11-25-25	0	16	16	1
Totals: 13 days	109	241	383	5

Totals:	13 days	109	241	383	5

Key Concepts

- **Per-Agent Allocation**

  Your SmartApps contract may include a set number of IVR minutes or SMS messages per licensed agent. These allocations establish your baseline usage limits for the billing period.

  > **Example:** 100 agents × 50 minutes = 5,000 total IVR minutes per month

- **Agents Logged In**

This metric shows the number of distinct agents who logged into SmartApps during the reporting period. Tracking active agent count alongside usage ensures accurate forecasting and license optimization.

It helps measure:

- Overall **system adoption and engagement**
- Correlation between **agent activity and communication volume**
- Identification of **inactive or underutilized licenses**

- **Overage Charges**

  If overall usage exceeds your allocated limits, additional overage charges apply at the contracted rate. This report highlights any overages, allowing you to manage capacity before they appear on your monthly bill.

- **Usage Breakdown**

  The report supports multiple viewing intervals:

  - **Daily or Weekly Trends:** to identify peak periods or campaign impacts
  - **Monthly Totals:** for high-level billing validation
  - **Custom Date Ranges:** for audits or performance reviews

- **Billing Validation**

  Use this report to cross-verify your SmartApps invoice from TTEC Digital. Aligning report data with billing ensures transparency, accuracy, and budget control.

- **System Integration**

  All IVR and SMS activity is processed through SmartApps' unified carrier network, ensuring consistent tracking and centralized reporting across all communication channels.

What you will see in the report

Field	Description
SMS Usage	Number of SMS messages sent (primarily for 2FA)
IVR Usage	Number of IVR call minutes used
Agents Logged In	The number of active agents who accessed SmartApps during the selected period. Reflects system utilization and staffing levels.
Usage Period	The start and end dates defining the reporting window.

Application

Use this report to:

- **Track** SMS, IVR, and agent activity over time.
- **Monitor** usage relative to contract allocations.
- **Identify** active agent participation and workload distribution.
- **Validate** monthly invoices and detect discrepancies.
- **Forecast** future usage and adjust allocations as your team or member activity grows.

> **Example:** A credit union sees a rise in IVR call minutes and SMS usage during tax season. Reviewing the Usage Summary Report shows a corresponding increase in "Agents Logged In," confirming higher agent engagement rather than system misuse. The operations team uses this insight to adjust staffing and usage allocations for the following quarter.

Tips for Users

- Run this report **monthly** to confirm active usage and prevent overage charges.
- Compare **Agents Logged In** to total licensed users to identify underutilized accounts.
- Review **daily or weekly views** for unusual spikes in IVR or SMS activity.
- Share findings with **finance and operations teams** for budgeting, contract planning, and staffing insights.
- Use **trend data** to forecast upcoming campaigns or seasonal usage fluctuations.

Summary

Proactive Info Summary report provides a consolidated view of how Proactive Info handles calls by presenting relevant account information to callers before they reach an agent, with the objective of resolving the interaction without agent involvement.

Description

The report measures the effectiveness of SmartApps in proactively delivering informational messages—such as balance details, recent transactions, alerts, or status notifications—while callers are in the queue or being processed. Calls are considered successfully handled when the caller receives the necessary information and disconnects without speaking to an agent. The report also captures authentication outcomes, event categories triggered, and the proportion of calls that continued to an agent despite proactive messaging.

> **Note:** Proactive Info is customer-focused (resolves needs before agent contact), in contrast to Screen Pop, which is agent-focused (prepares data for an agent once a transfer is triggered).

Key Concepts

- **Proactive Information Delivery**

  The system plays tailored information—e.g., balances, delinquency alerts, posted deposits—intended to answer common inquiries without agent engagement.

- **Successful Call Resolution**

  A call is treated as successfully handled when the caller receives information and terminates the call before agent transfer.

- **Containment and Efficiency**

  Proactive Info reduces the number of calls requiring agent assistance and decreases handling time on calls that do reach agents, contributing to operational efficiency.

- **Event Categories**

  The system may deliver information tied to conditions such as Collections, Delinquency, Dormancy, Frozen status, or transactional summaries.

What you will see in the report

Field	Description
Utilization Metrics	Total calls received, total using Proactive Info, and percentage utilization.
Events Summary	Counts of callers who heard balance info, transaction info, posted deposits, withdrawals, or custom informational messages.
Condition-Based Alerts	Counts of calls where conditions such as Collections, Delinquency, Dormancy, Frozen, Bankruptcy, or Other Alerts applied.
Authentication Summary	Number and percentage of calls successfully authenticated or not authenticated during proactive processing.
Outcome Metrics	Calls that disconnected after hearing info vs. calls that proceeded to an agent.
Member Identification via Phone Number	Indicates whether the caller was located in member records and if authentication succeeded thereafter.
Time Comparison	Difference in handling time between calls with proactive information and those without.

Application

Use this report to:

- **Determine** how effectively proactive content deflects calls from agents.
- **Identify** informational categories most frequently resolving calls without agent involvement.
- **Evaluate** authentication success within proactive processing.

- **Detect** conditions or alerts that frequently influence call outcomes.
- **Quantify** operational savings associated with proactive containment (time and agent reduction).

> **Example:** If a high proportion of callers hearing posted deposits or balance information hang up without agent interaction, the institution can validate that Proactive Info is achieving its intended business outcome.

Tips for Users

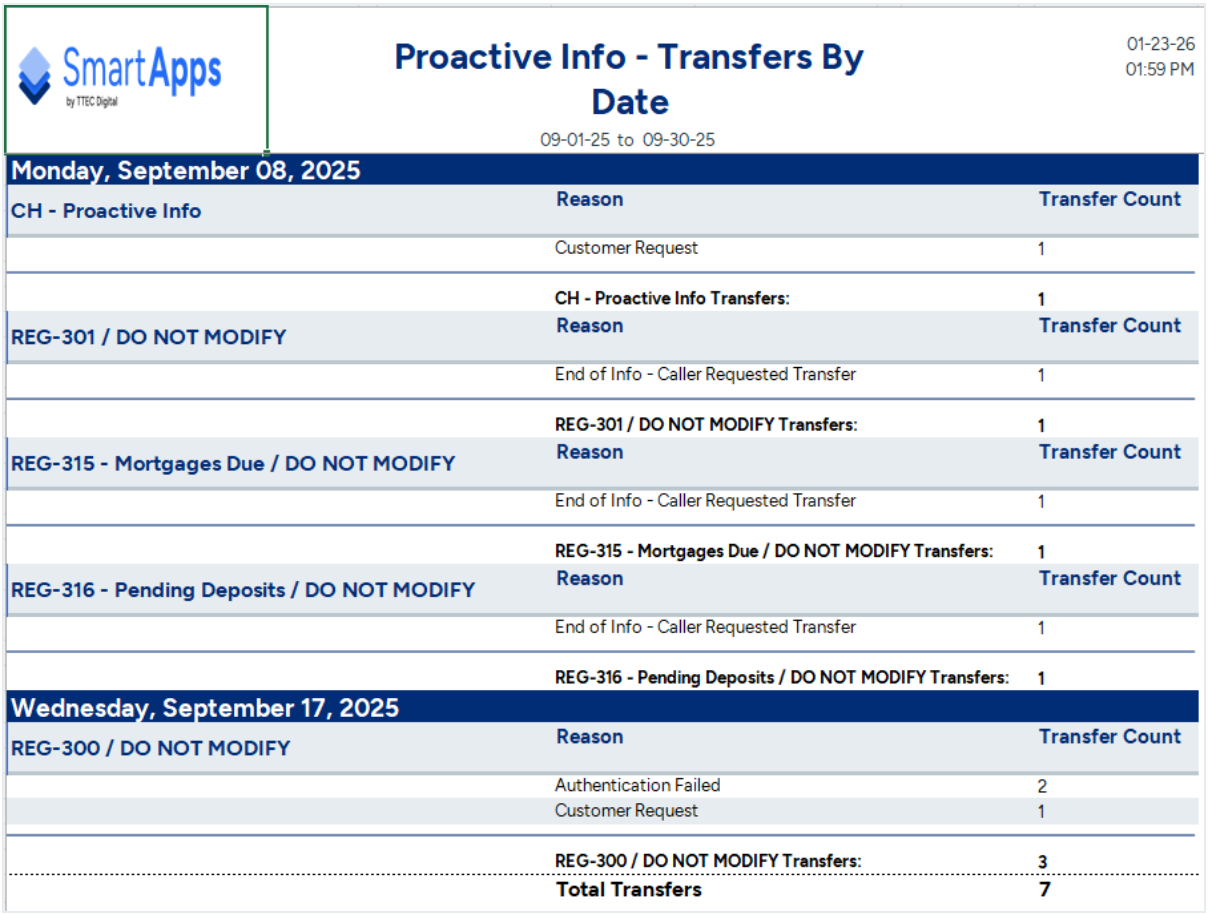
- Review after script or logic changes that affect proactive messaging or alert conditions.
- Compare containment percentages before and after adjustments to messaging wording or order.
- Monitor which informational categories most strongly correlate with self-resolution to prioritize improvements.
- Share results with operations leadership to demonstrate efficiency gains attributed to Proactive Info.
- Use in conjunction with Screen Pop Transfer reports to understand the division between self-served and agent-assisted call outcomes.

Transfer By Date

Description

The Proactive Info - Transfer by Date report identifies interactions that were not fully resolved through proactive messaging and therefore required escalation to an agent. Transfers are displayed by date and by Proactive Info Profile, with counts assigned to the specific reasons that triggered the agent hand-off. This allows institutions to analyze when and why proactive containment did not occur and to determine whether failures are systemic, time-based, or tied to particular informational events or caller behaviors.

> **Note:** This report provides a daily breakdown of calls that exited Proactive Info and were transferred to an agent, grouped by Proactive Info Profile and categorized by the reason for transfer.



SmartApps by TTEC Digital

Proactive Info - Transfers By Date

09-01-25 to 09-30-25

01-23-26
01:59 PM

Monday, September 08, 2025		
CH - Proactive Info	**Reason**	**Transfer Count**
	Customer Request	1
	CH - Proactive Info Transfers:	**1**
REG-301 / DO NOT MODIFY	**Reason**	**Transfer Count**
	End of Info - Caller Requested Transfer	1
	REG-301 / DO NOT MODIFY Transfers:	**1**
REG-315 - Mortgages Due / DO NOT MODIFY	**Reason**	**Transfer Count**
	End of Info - Caller Requested Transfer	1
	REG-315 - Mortgages Due / DO NOT MODIFY Transfers:	**1**
REG-316 - Pending Deposits / DO NOT MODIFY	**Reason**	**Transfer Count**
	End of Info - Caller Requested Transfer	1
	REG-316 - Pending Deposits / DO NOT MODIFY Transfers:	**1**
Wednesday, September 17, 2025		
REG-300 / DO NOT MODIFY	**Reason**	**Transfer Count**
	Authentication Failed	2
	Customer Request	1
	REG-300 / DO NOT MODIFY Transfers:	**3**
	Total Transfers	**7**

Key Concepts

- **Proactive Transfer Event**

  A call that received proactive messaging but continued to an agent due to caller request, authentication issues, or other conditions.

- **Proactive Info Profile**

  A configuration grouping that governs which proactive information is played (e.g., balances, pending deposits, due payments, condition alerts).

- **Transfer Reasons**

  Transfers represent containment failures in proactive handling. Common triggers include:

- End of Info: Caller Requested Transfer
- Authentication Failure
- Customer Request
- Collections / Delinquency / Condition-Based Routing

What you will see in the report

Field	Description
Date	The specific day on which the transfer occurred.
Proactive Info Profile	The configured profile that managed the call before transfer.
Reason	The stated cause for escalation to an agent.
Transfer Count	Number of calls transferred for that reason under that profile on that date.
Daily Profile Totals	Total transfers per profile per date.
Grand Total	Total transfers across all profiles and dates in the selected range.

Application

Use this report to:

- **Identify** days with unusual increases in agent transfers following proactive attempts.
- **Determine** which Proactive Info Profiles are least effective at containing calls.
- **Correlate** transfer causes with specific informational categories or caller behaviors.

- **Validate** whether condition-based alerts (e.g., delinquency or pending payments) are correctly triggering transfers rather than resolving calls.
- **Monitor** the effectiveness of proactive interventions after configuration or messaging changes.

> **Example:** If multiple profiles show "End of Info – Caller Requested Transfer" as the dominant reason on the same date, messaging clarity or sequence may require review.

Tips for Users

- Review this report in conjunction with the **Proactive Info – Summary report** to connect transfer events with overall utilization and containment.
- Prioritize investigation of repeated transfer causes linked to the same profile across multiple dates.
- **Reassess** scripting or message order if customers consistently request transfer after hearing full proactive content.
- Use this report after proactive content or campaign changes to verify whether transfers decrease or persist.

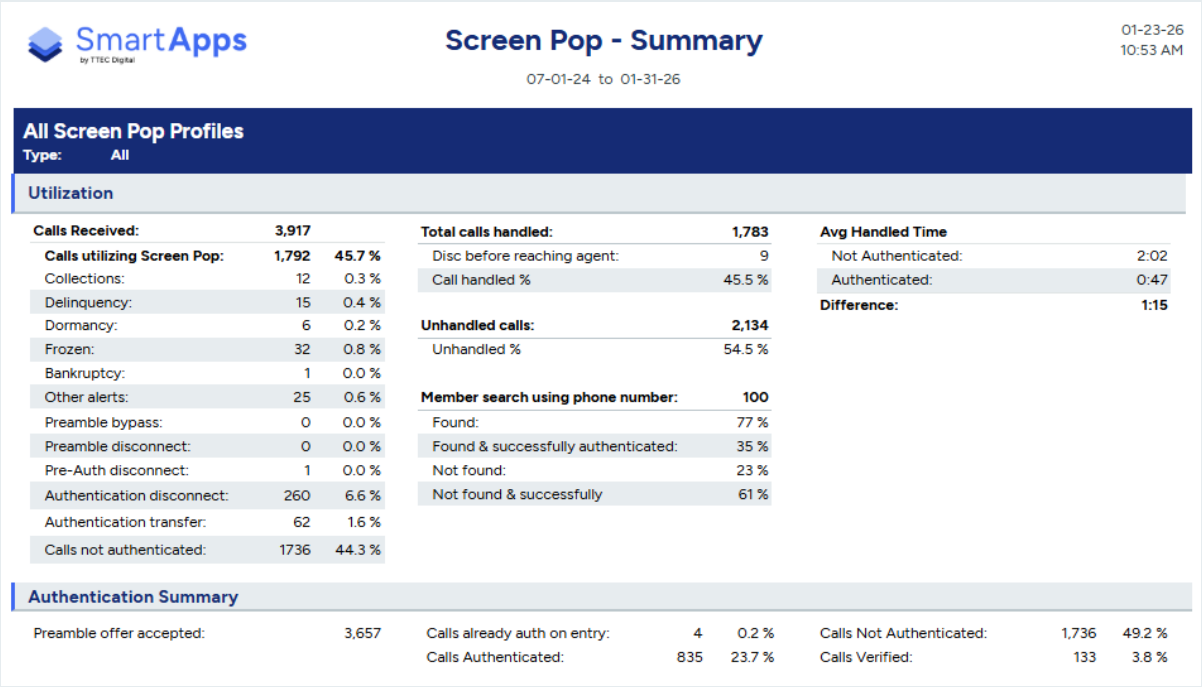
Summary

Description

The Screen Pop Summary Report measures how effective different call routes are at identifying callers before they reach an agent.

A route is considered successful when it collects enough information to identify the caller (like a member number, PIN, or phone number) - and upon connecting to an agent. The member's information/details are automatically displayed on the agent's screen.

> **Note:** Identify callers as early as possible so agents spend less time verifying details and more time resolving issues.



SmartApps by TTEC Digital

Screen Pop - Summary

07-01-24 to 01-31-26

01-23-26
10:53 AM

All Screen Pop Profiles
Type: All

Utilization

Calls Received:	**3,917**	
Calls utilizing Screen Pop:	**1,792**	**45.7 %**
Collections:	12	0.3 %
Delinquency:	15	0.4 %
Dormancy:	6	0.2 %
Frozen:	32	0.8 %
Bankruptcy:	1	0.0 %
Other alerts:	25	0.6 %
Preamble bypass:	0	0.0 %
Preamble disconnect:	0	0.0 %
Pre-Auth disconnect:	1	0.0 %
Authentication disconnect:	260	6.6 %
Authentication transfer:	62	1.6 %
Calls not authenticated:	1736	44.3 %

Total calls handled:	**1,783**
Disc before reaching agent:	9
Call handled %	45.5 %
Unhandled calls:	**2,134**
Unhandled %	54.5 %
Member search using phone number:	**100**
Found:	77 %
Found & successfully authenticated:	35 %
Not found:	23 %
Not found & successfully	61 %

Avg Handled Time	
Not Authenticated:	2:02
Authenticated:	0:47
Difference:	**1:15**

Authentication Summary

Preamble offer accepted:	3,657	Calls already auth on entry:	4	0.2 %	Calls Not Authenticated: 1,736 49.2 %
		Calls Authenticated:	835	23.7 %	Calls Verified: 133 3.8 %

Key Concepts

- **Screen Pop**

  When a call arrives, the system identifies the caller and instantly “pops” their member information onto the agent’s screen. A successful screen pop reduces agent handle time and improves member experience.

- **Authentication Types**

  - Each route can be analyzed by its success rate for authentication. High failure rates may suggest overly complex authentication steps, missing data, or poor pre-authentication coverage.
  - **Authenticated Route:** Caller provides info (e.g., member number, PIN) to confirm identity before routing to an agent.
  - **Pre-Authenticated Route:** Caller is already identified earlier in the process (e.g., through phone number look-up or authenticating in another upstream product).

  Routes and Profiles

  Route: The path a call takes to enter the financial institution’s system - each route has a Screen Pop Profile asigned/configured.
  Profile: The logic defining how the system manages and authenticates each call for a given route.

> **Example:** Calls where the caller enters authentication info (like member number or PIN). Calls where the caller is pre-authenticated (already identified earlier by phone number or other SmartApps tools).

What you will see in the report

Field	Description
Utilization	
Calls Received	The number of calls which entered Screen Pop
Calls utilizing Screen Pop	The number of calls which were successfully authenticated/identified and continued on to queue (did not bypass, disconnect, or exception routing transfer out)
Collections	The number of calls identified as in Collections and transferred (Exception Routing)
Delinquency	The number of calls identified as in Delinquency and transferred (Exception Routing)
Dormancy	The number of calls identified as in Dormancy and transferred (Exception Routing)
Frozen	The number of calls identified as Frozen and transferred (Exception Routing)
Bankruptcy	The number of calls identified as in Collections and transferred (Exception Routing)
Other Alerts	The number of calls having Core Alert Codes and transferred (Exception Routing)
Preamble Bypass	The number of calls that selected the "Bypass" option in the Preamble menu (opted to NOT enter any authentication/identification info)
Preamble Disconnect	The number of callers who disconnected at the Preamble menu
Pre-Auth Disconnect	The number of callers who disconnected at the Pre-Authentication message
Authentication Disconnect	The number of callers who disconnected in Authentication
Authentication Transfer	The number of callers who transferred while in Authentication process
Calls not Authenticated	The number of callers who continued on to queue Not Authenticated (failed Authentication)

Field	Description
Total calls handled	The number of calls which were successfully authenticated/identified and continued on to queue
Disc before reaching agent	Number of calls disconnecting in Screen Pop
Calls handled %	Percentage of calls which were successfully authenticated/identified and continued on to queue
Unhandled calls	Number of calls which exception transferred out of or disconnecting in Screen Pop
Unhandled %	Percentage of calls which exception transferred out of or disconnecting in Screen Pop
Member search using phone number	Number of calls where Phone Number search was attempted
Found	Number of calls found/identified via Phone Number search
Found & successfully Authenticated	Number of calls found/identified via Phone Number search AND successfully Authenticated
Not found	Number of calls not found/identified via Phone Number search
Not found & successfully	Number of calls not found/identified via Phone Number search AND successfully Authenticated
Average Handled Time Not Authenticated"	Average time agents spend on Not Authenticated calls
Average Handled Time Authenticated"	Average time agents spend on Authenticated calls
Difference	the difference between the Average Handle Times above
Authentication Summary	
Preamble offer accepted	The number of calls that selected the "continue" option (to enter Authentication) in the Preamble menu
Calls already auth on entry	Number of calls who came into Screen Pop 'Authenticated' (had successfully Authenticated in an upstream product)
Calls Authenticated	Number of calls who successfully Authenticated and con-

Field	Description
	tinued to queue
Calls not Authenticated	The number of callers who continued on to queue Not Authenticated (failed Authentication)
Calls Verified	Number of calls who were not able to successfully complete atthentication and continued to queue in 'Verified' status (Verified meaning partially Authenticated)

Application

Use this report to:

- **Identify** which routes most effectively authenticate callers.
- **Detect** routes with high authentication failure or longer handle times.
- **Benchmark** AHT improvements after IVR optimization.
- **Support** data-driven refinements to IVR scripts or authentication prompts.

> **Example:** If 70% of calls on the “Loan Inquiry” route fail authentication, the credit union can review the prompt wording or authentication logic to reduce friction.

Tips for Users

- Run this report after **IVR or authentication-script updates** to confirm effectiveness.
- Review it alongside the Screen Pop Transfer by Date report to spot daily trends.
- Share it with contact-center managers and SmartApps admins to guide route-level improvements.
- Compare **pre- and post-update AHT averages** to quantify efficiency gains.

Transfer By Date

Description

This report identifies the 'transfer reason' for calls that transferred to an agent from within Smart Screen Pop. Each transfer is grouped by the Screen Pop Profile that handled the call and is summarized by the reason for transfer and total transfer counts per day.

Transfers in this report represent points where calls were intentionally routed to agent for specific scenarios (Failed Authentication, Collections, Bankruptcy, etc) , making it a key tool for identifying breakdowns in self-service and validating routing logic.

SmartApps by TTEC Digital

Screen Pop - Transfers By Date

07-01-24 to 07-01-24

01-23-2(
12:16 PM

July 01, 2024

CH - Screen Pop	Reason	Transfer Count
	Authentication Failed	3
	CH - Screen Pop Transfers:	**3**

REG-100 / DO NOT MODIFY	Reason	Transfer Count
	Authentication Failed	3
	Customer Request	1
	REG-100 / DO NOT MODIFY Transfers:	**4**

REG-112 / DO NOT MODIFY	Reason	Transfer Count
	Customer Request	2
	Authentication Failed	2
	REG-112 / DO NOT MODIFY Transfers:	**4**

REG-160 / DO NOT MODIFY	Reason	Transfer Count
	Customer Request	6
	Authentication Failed	3
	REG-160 / DO NOT MODIFY Transfers:	**9**

REG-161 / DO NOT MODIFY	Reason	Transfer Count
	Authentication Failed	1
	REG-161 / DO NOT MODIFY Transfers:	**1**

REG-162 / DO NOT MODIFY	Reason	Transfer Count
	Authentication Failed	1
	REG-162 / DO NOT MODIFY Transfers:	**1**

REG-163 / DO NOT MODIFY	Reason	Transfer Count
	Authentication Failed	1
	REG-163 / DO NOT MODIFY Transfers:	**1**

REG-185 / DO NOT MODIFY	Reason	Transfer Count
	Customer Request	3
	REG-185 / DO NOT MODIFY Transfers:	**3**

Key Concepts

- **Screen Pop Profile**: A defined call-handling logic path (e.g., CH – Screen Pop, REG-100) that determines how callers are authenticated and routed before reaching an agent.
- **Transfer Event**:A call hand-off from SmartApps to an agent due to an inability to complete authentication, business rules, or caller intent.
- **Transfer Reasons**: Common triggers include:
    - Authentication Failed: caller failed identity verification
    - Customer Request: caller explicitly chose to speak to an agent
    - Account Exceptions: delinquency, collections, or frozen status

What you will see in the report

Field	Description
Date	The calendar day on which the transfers occurred.
Screen Pop Profile	The Screen Pop profile that routed the call before transfer.
Reason	The (Transfer) Reason/Category the call is transferring to an agent under.
Transfer Count	The number of calls transferred for that specific reason and profile on that date.
Daily Total (per profile)	Sum of all transfer reasons within that profile for that day.
Grand Total	Total transfers across all profiles and reasons within the date range.

Application

Use this report to:

- **Identify** profiles or flows with high transfer volume.
- **Detect** authentication failures that may be corrected through script or logic adjustment.
- **Validate** that transfers caused by policy (e.g., collections, fraud) occur as expected.
- **Measure** the impact of IVR or routing changes by comparing transfer frequency before and after deployment.
- **Support** queue management by understanding which flows generate agent workload.

> **Example:** A high rate of "Authentication Failed" transfers within a specific profile may indicate unclear prompts, expired credentials, or missing data feeds, prompting review of authentication design.

Tips for Users

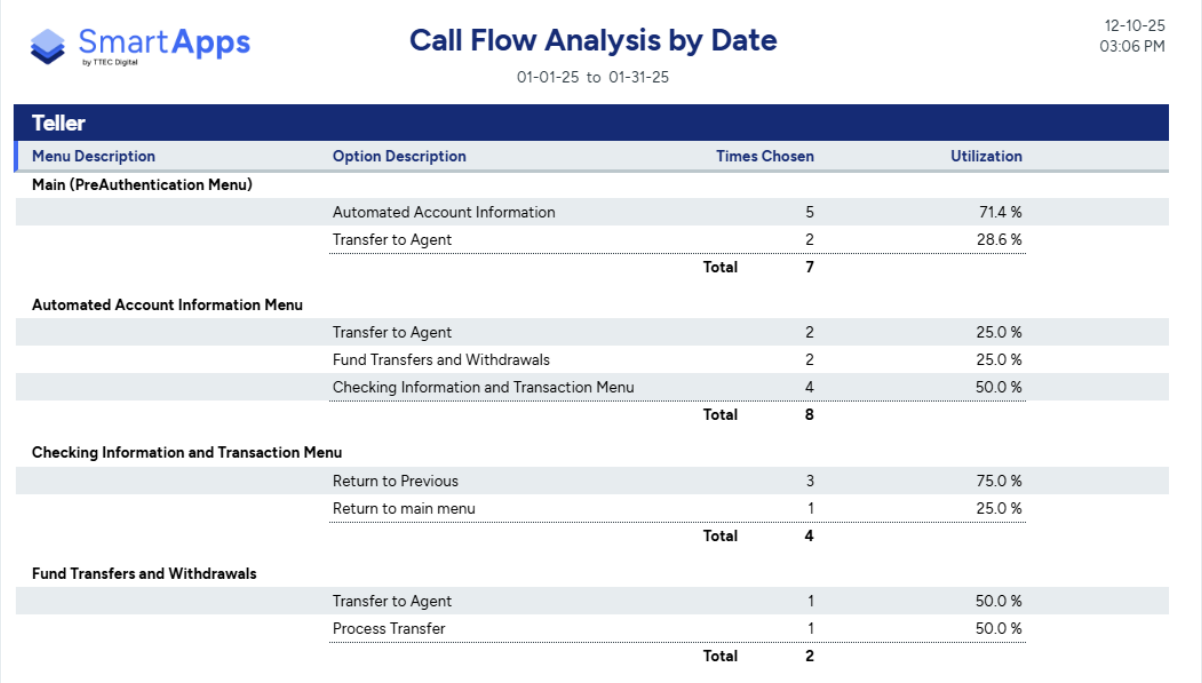
- Review this report following modifications to authentication, routing, or messaging to verify intended outcomes.
- Prioritize investigation of avoidable transfers (e.g., authentication failures, unclear scripting) before intentional transfers (e.g., collections enforcement).
- Cross-reference with the Screen Pop Summary report to correlate transfer reasons with identification success rates.
- Share findings with contact center management and SmartApps administrators to drive corrective actions.

Call Flow Analysis

Description

The Call Flow Analysis report measures caller behavior within Teller(IVR) menus by tracking which menu options were selected, how many callers advanced through a flow, returned to a prior menu, ended the call, or transferred to an agent. The report displays interaction volumes and percentage utilization for each option at every IVR menu level.

This report is used to understand how members navigate IVR menus, which self-service options are used most often, and where callers disengage or escalate to live assistance .



SmartApps by TTEC Digital

Call Flow Analysis by Date

01-01-25 to 01-31-25

12-10-25
03:06 PM

Teller

Menu Description	Option Description	Times Chosen	Utilization
Main (PreAuthentication Menu)			
	Automated Account Information	5	71.4 %
	Transfer to Agent	2	28.6 %
	Total	**7**	
Automated Account Information Menu			
	Transfer to Agent	2	25.0 %
	Fund Transfers and Withdrawals	2	25.0 %
	Checking Information and Transaction Menu	4	50.0 %
	Total	**8**	
Checking Information and Transaction Menu			
	Return to Previous	3	75.0 %
	Return to main menu	1	25.0 %
	Total	**4**	
Fund Transfers and Withdrawals			
	Transfer to Agent	1	50.0 %
	Process Transfer	1	50.0 %
	Total	**2**	

Key Concepts

- **Call Flow / Menu Path**

  A defined IVR route that controls what options a caller can access (for example: Mortgage Information and Transaction Menu, Fund Transfers, Card Block, or Checking Information). Some menus are available pre-authentication, while others require account login.

- **Flow-Level Actions**

  Each menu records the specific action taken by the caller, such as:

  - Account balances
  - Make a loan or mortgage payment
  - Process a transfer
  - Repeat menu
  - Return to main menu
  - Transfer to agent
  - End the call

- **Outcome Distribution**

  For each call flow and date, the report shows:

  - Action count : number of times an option was chosen
  - Utilization percentage : distribution across options within the flow

- **Usage Insight**

  Patterns such as high Transfer to Agent, Return to Main Menu, or End the Call selections can indicate:

  - Confusing prompts
  - Missing self-service options

- Excessive menu depth
- Information that callers expect but cannot find

What you will see in the report

Field	Description
Date	The calendar day the call activity occurred
Call Flow Name	The self-service function or IVR menu path the caller entered (for example, Checking Information, Mortgage Information, or Transaction Menu).
Option / Description	The action selected by the caller within that menu
Times Chosen	Number of times that option was selected
Utilization %	Percent distribution of selections within that flow
Totals	Total interactions for the menu on that date
Report Date/Time	Timestamp indicating when the report was generated

Application

Use this report to:

- Identify which IVR menus and self-service functions receive the highest usage
- Detect call flows with high agent transfers or frequent returns to main menu
- Measure containment effectiveness of transactional flows (payments, transfers, balance inquiries)
- Pinpoint menus that may require redesign, rewording, or reordering
- Validate whether callers are successfully completing actions (e.g., payments processed vs. canceled)

> **Example:** If 125 callers entered “Main” but only 79 reached any sub-action, the gap may indicate unclear prompts or poor menu labeling.

Tips for Users

- Compare menus with high abandonment to wording or depth of options.
- Combine with **Transfers-by-Destination** to understand escalation points.
- Review after IVR wording or structure changes to measure impact.
- Use trends over time to detect stability or degradations in experience.
- Review “Return to Main Menu” volume as usability feedback

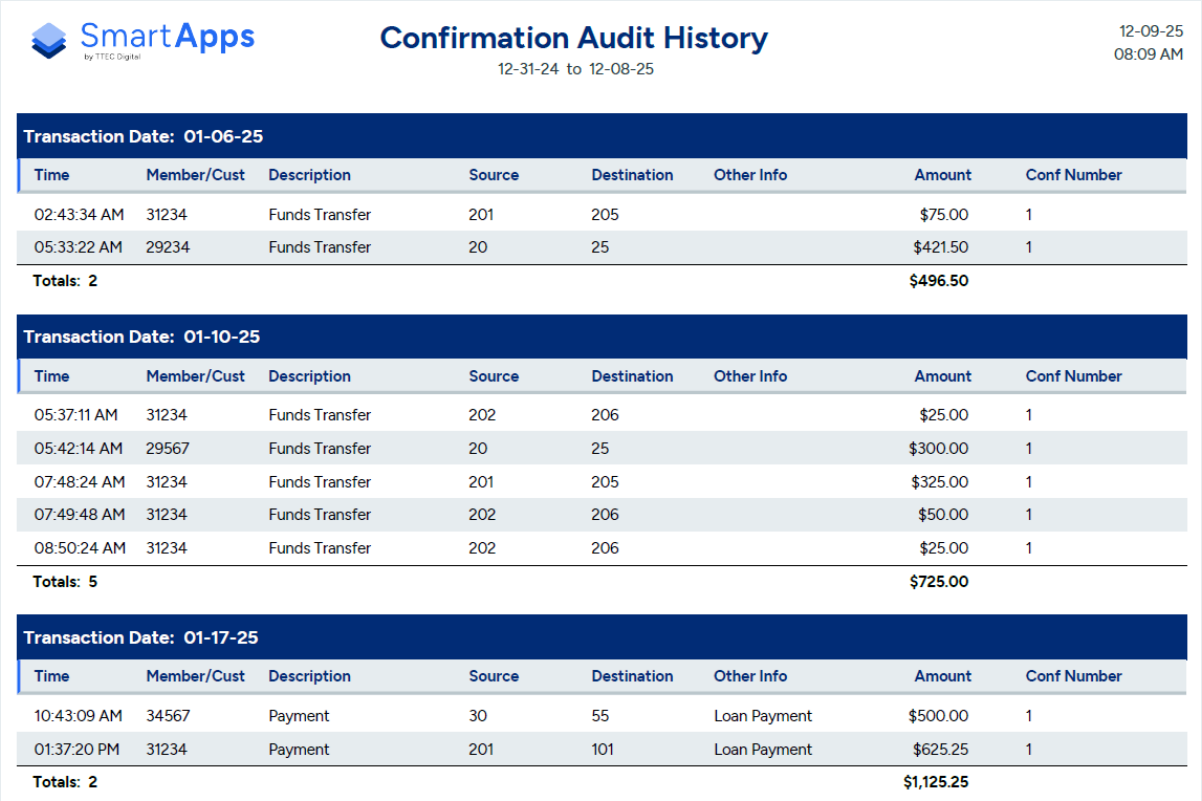
Confirmation Audit History

Description

The Confirmation Audit History report captures **completed transactions executed by members through IVR**. Each entry represents an action that was successfully submitted to the core system and acknowledged with a confirmation identifier.

The report includes both **financial** and **non-financial** IVR actions—such as payments, funds transfers, stop payments, card actions, and withdrawals and records detailed transaction attributes including date/time, source and destination accounts, posted amounts, and confirmation numbers.

Transactions are grouped **by transaction date**, creating a chronological audit trail of member-initiated activity executed through IVR/SmartApps. This report serves as an operational and historical reference and is not limited to formal audit or reconciliation use cases



SmartApps by TTEC Digital

Confirmation Audit History

12-31-24 to 12-08-25

12-09-25
08:09 AM

Transaction Date: 01-06-25

Time	Member/Cust	Description	Source	Destination	Other Info	Amount	Conf Number
02:43:34 AM	31234	Funds Transfer	201	205		$75.00	1
05:33:22 AM	29234	Funds Transfer	20	25		$421.50	1
Totals: 2						**$496.50**	

Transaction Date: 01-10-25

Time	Member/Cust	Description	Source	Destination	Other Info	Amount	Conf Number
05:37:11 AM	31234	Funds Transfer	202	206		$25.00	1
05:42:14 AM	29567	Funds Transfer	20	25		$300.00	1
07:48:24 AM	31234	Funds Transfer	201	205		$325.00	1
07:49:48 AM	31234	Funds Transfer	202	206		$50.00	1
08:50:24 AM	31234	Funds Transfer	202	206		$25.00	1
Totals: 5						**$725.00**	

Transaction Date: 01-17-25

Time	Member/Cust	Description	Source	Destination	Other Info	Amount	Conf Number
10:43:09 AM	34567	Payment	30	55	Loan Payment	$500.00	1
01:37:20 PM	31234	Payment	201	101	Loan Payment	$625.25	1
Totals: 2						**$1,125.25**	

Key Concepts

- **Channel-Confirmed Transactions**

  The only transactions that are included in this report are:

  - Initiated through SmartApps IVR, and
  - Successfully submitted to and acknowledged by the core system

  Failed, abandoned, or incomplete IVR attempts do not appear.

- **Financial and Non-Financial Activity**

  - Examples of financial actions:

    - Loan Payments
    - Mortgage Payments

        - Credit Card Payments
        - Funds Transfers
        - Withdrawals
        - Member-to-Member Transfers
    - Examples of non-financial actions:
        - Stop Payments
        - PIN Changes
        - Card Operations (activation/ blocking when included)

- **Confirmation Number**

  Each transaction includes a confirmation identifier:

    - If returned by the core, the core confirmation is displayed.
    - If the core does not supply one, **SmartApps generates a unique confirmation** prefixed with **SA** to maintain traceability.

- **Date Grouping**

  Transactions are grouped under **Transaction Date** headers, with a daily subtotal shown after each date block.

> **Note:** Non-financial actions display a $0.00 amount but still generate confirmation entries.

What you will see in the report

Field	Description
Tran Date/ time	Exact timestamp when the action was submitted
Member/ Customer	Member or customer number associated with the transaction.

Field	Description
Description	Transaction type (e.g., Payment, Funds Transfer, Withdrawal, Stop Payment).
Source	The account or instrument the funds/ action originated from (e.g., share ID, loan ID, checking suffix).
Destination	The account or instrument receiving the payment/ transfer when applicable.
Other Info	Supplementary information such as “Loan Payment”, “Mortgage Payment”, or “Check: ####” on stop payments.
Amount	Dollar value for financial transactions; will show $0.00 for non-financial items (e.g., Stop Payments).
Conf Number	Confirmation number returned from the core or generated by SmartApps (SA-prefixed if system-generated).
Daily Total Line	Appears under each date block, showing total number of transactions and combined dollar amount for that date.
Report Totals	Final summary showing total volume and dollar value for the date range

Application

Use this report to:

- **Validate** that IVR-initiated transactions posted successfully to core.
- **Review** member-performed activity for operational transparency and traceability.
- **Investigate** a reported member transaction using confirmation details.
- **Verify** totals for volume-aware planning or trend observation.
- **Support** audit trail requirements for digitally-submitted actions.

> **Example:** A stop payment dispute or loan payment inquiry can be traced using the exact date, source/ destination, and confirmation value found in the report.

Tips for Users

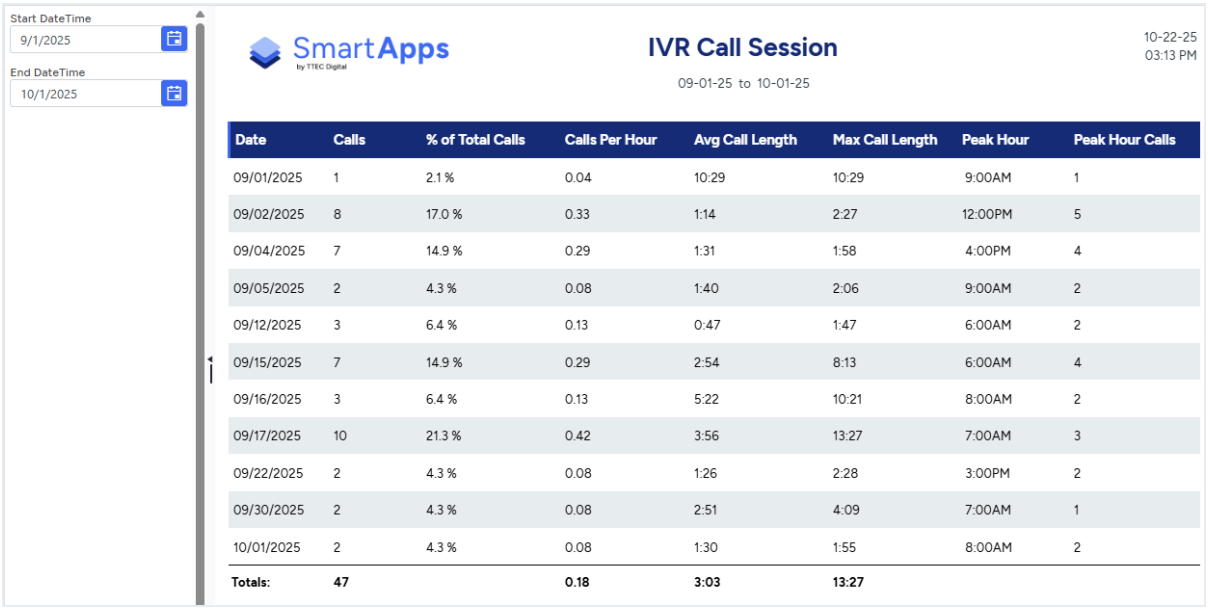
- When investigating member claims (e.g., “I made a payment by phone”), search by **transaction date** and **confirmation number**.
- Review non-financial actions (e.g., multiple stop payments at $0.00) to detect potential repeat misuse or error patterns.
- Use totals to monitor **volume shifts over time** following product changes or IVR routing adjustments.
- Combine with **Monetary Transaction** or **Transfer by Destination** reports to compare channel usage behaviors.

IVR Call Session

Description

The IVR Call Session report captures daily totals of calls interacting with the Smart Teller system, regardless of whether the calls completed self-service or transferred out to an agent. For each date, the report shows overall call volume, proportion of total traffic, hourly call density, and session duration patterns. The report also identifies the highest-traffic hour of the day and the number of calls in that hour, supporting operational and capacity planning.

This report provides a date-based summary of calls that entered the IVR (Smart Teller) system, including calls that disconnected within IVR and those that eventually continued to the contact center. It reflects actual system usage and call duration characteristics over the selected time range.



Start DateTime
9/1/2025
End DateTime
10/1/2025

SmartApps by TTEC Digital

IVR Call Session

09-01-25 to 10-01-25

10-22-25
03:13 PM

Date	Calls	% of Total Calls	Calls Per Hour	Avg Call Length	Max Call Length	Peak Hour	Peak Hour Calls
09/01/2025	1	2.1 %	0.04	10:29	10:29	9:00AM	1
09/02/2025	8	17.0 %	0.33	1:14	2:27	12:00PM	5
09/04/2025	7	14.9 %	0.29	1:31	1:58	4:00PM	4
09/05/2025	2	4.3 %	0.08	1:40	2:06	9:00AM	2
09/12/2025	3	6.4 %	0.13	0:47	1:47	6:00AM	2
09/15/2025	7	14.9 %	0.29	2:54	8:13	6:00AM	4
09/16/2025	3	6.4 %	0.13	5:22	10:21	8:00AM	2
09/17/2025	10	21.3 %	0.42	3:56	13:27	7:00AM	3
09/22/2025	2	4.3 %	0.08	1:26	2:28	3:00PM	2
09/30/2025	2	4.3 %	0.08	2:51	4:09	7:00AM	1
10/01/2025	2	4.3 %	0.08	1:30	1:55	8:00AM	2
Totals:	**47**		**0.18**	**3:03**	**13:27**		

Key Concepts

- **IVR Usage Coverage**

  Every call that entered Smart Teller is included, whether it disconnected in IVR or transitioned to the contact center.

- **Total Calls**

  Indicates the total number of calls processed through the IVR system during the selected period. For example, on October 24th, 2024 the system recorded 46 total calls.

- **Percent of Total Calls**

  Represents the percentage of calls received on a specific day compared to the overall calls for the report's time range. Example: If 46 calls were received on October 24th and the total for the selected period was 164 calls, the percentage would be 28%.

- **Calls Per Hour**

  Average number of calls processed by the IVR system per hour over a 24-hour period. Example: With 46 calls in 24 hours, the calls-per-hour metric would be ~1.92 calls per hour.

- **Average Call Length**

  The average duration of a call during the selected period. Example: If the average call length is 1 minute and 52 seconds, this reflects the average time users spent interacting with the IVR.

- **Maximum Call Length**

  The duration of the longest call during the selected period. Example: The longest call might have lasted 4 minutes and 36 seconds.

- **Peak Hour**

  Identifies the hour of the day when the highest volume of calls occurred. Example:

If 15 calls were received at 10:00 AM, this would be flagged as the peak hour for that day.

What you will see in the report

Field	Description
Date	The calendar date on which IVR sessions occurred.
Calls	Number of calls that interacted with Smart Teller on that date.
% of Total Calls	Portion of total IVR calls represented by that day for the reporting period.
Calls Per Hour	Average hourly call rate calculated across a 24-hour period.
Avg Call Length	Mean duration of calls handled by IVR for that day.
Max Call Length	Longest single IVR session recorded on that date.
Peak Hour	Hour of day with the highest call volume (e.g., 7:00 AM, 2:00 PM).
Peak Hour Calls	Number of calls received during that peak hour.
Totals	Sum of calls across the date range and overall averages.

Application

Use this report to:

- **Evaluate** IVR utilization over time and confirm system adoption.
- **Identify** peak periods to inform staffing, overflow routing, or maintenance scheduling.
- **Detect** unusual call-length patterns that may indicate menu friction or caller confusion.

- **Support** capacity planning for voice infrastructure and trunk utilization.
- **Monitor** usage trends following script, routing, or promotional changes.

> **Example:** If the peak hour consistently occurs between 6–8 AM, staffing or proactive messaging can be aligned to that window.

Tips for Users

- Compare the peak hour trends against transfer or containment reports to understand where demand converts to agent load.
- Monitor average call length following IVR menu redesigns or prompt adjustments.
- Investigate days with abnormal spikes or unusually long sessions to identify root causes (campaigns, outages, or system changes).
- Use this report as a baseline before deploying new call flows or authentication strategies.

Menu Sequence

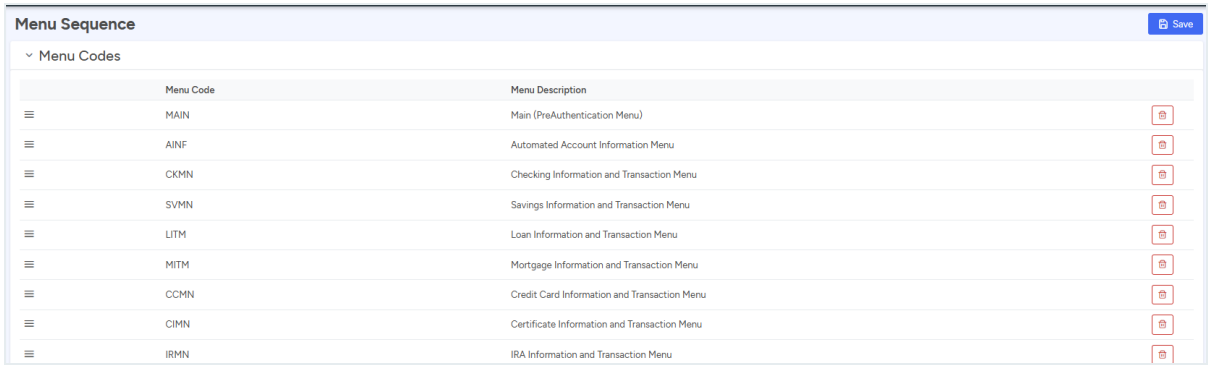
Description

By default, Teller menus may appear in reports in an order that does not reflect the actual IVR journey (e.g., alphabetical or based on internal codes). The Menu Sequence tool allows an administrator to drag and reposition menus so they appear in a logical, IVR-journey order.

> **Example:** Main → Automated Account Information → Checking Information → Transfers → Exit

This does not alter how the IVR behaves functionally. It strictly controls how reports are organized, particularly the **Call Flow Analysis** report. The Menu Sequence screen controls the display order of Teller menus in reporting, ensuring that call-flow based reports appear in the same logical order that members experience inside the IVR, instead of alphabetical or code-based order.

> **Note:** Credit union administrators cam reorder menus using this screen if they need to align report presentation with expected user flow or adjust after adding a new menu.



Key Concepts

- **Menu Code**

  Internal identifier for a specific menu entry.

- **Menu Description**

  Human-readable title displayed in configuration lists to describe the function of the menu.

- **Report-Only Impact**

  Reordering does not modify IVR routing logic or system behavior — it affects presentation only.

- **Drag-and-Drop Editing**

  Admins can reorder items interactively; changes apply immediately to reports.

- **One-Time Setup**

  Once the correct order is set, changes are rarely needed except when new menus are added.

What you will see in the report

Field	Description
Menu List (left panel)	Displays all teller menu items configured in the system.
Drag Handles	Used to reposition menus in desired order.
Description	Display label used to identify the menu in the configuration UI.

Application

Use this report to:

- **Position** a newly-added Teller menu correctly so reports reflect the correct journey order.
- **Correct** reports that appear in an illogical order when reviewing call flows.
- **Validate** or realign menu order during on-boarding, testing, or configuration reviews.

Tips for Users

- Arrange in the same order as callers actually experience menus in the IVR.
- Do not rely on alphabetical or code-based order but structure by journey.
- After reordering, run a Call Flow Analysis report to confirm desired view.
- Avoid frequent edits and adjust only when menu structure changes.

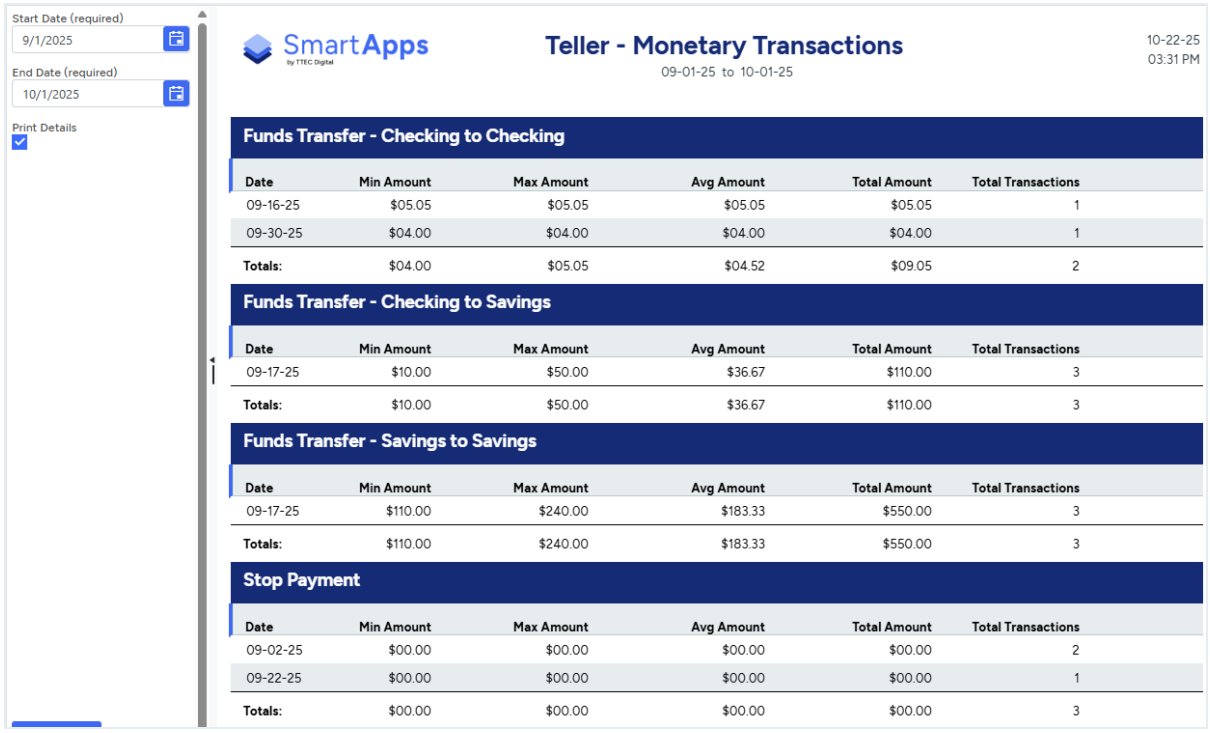
Monetary Transactions

Description

The Teller – Monetary Transactions report aggregates completed financial actions initiated in SmartApps Teller flows. For each transaction category, the report lists each date on which activity occurred and summarizes minimum, maximum, average, and total dollar amounts as well as the number of transactions for that date. A totals row is provided per category for the selected range.

This report provides a date-based summary of teller-initiated monetary actions completed through SmartApps (Teller module). Results are grouped by transaction category (e.g., Funds Transfer – Checking to Checking) and show daily amounts and volumes.

> **Note:** In this report, "Monetary Transactions" refers to posted financial actions in Teller flows (e.g., transfers and stop payments), not a cash-drawer reconciliation view. It is designed for volume/ amount monitoring by transaction category rather than per-teller cash balancing.



Key Concepts

- **Transaction Category**

  Logical grouping that reflects the Teller flow and direction of funds (e.g., *Funds Transfer – Checking to Checking*, *Funds Transfer – Checking to Savings*, *Funds Transfer – Savings to Savings, Stop Payment)*. Categories shown depend on enabled Teller features.

- **Daily Summaries**

  For each category and calendar date, the report summarizes the range and distribution of amounts and the total count of completed transactions.

- **Category Totals**

  A totals row under each category aggregates all dates in the selected range.

What you will see in the report

Field	Description
Category Header	The Teller transaction grouping (e.g., Funds Transfer – Checking to Checking, Funds Transfer – Checking to Savings, Funds Transfer – Savings to Savings, Stop Payment).
Date	Calendar date on which transactions in that category occurred.
Min Amount	Lowest single transaction amount for that category on that date.
Max Amount	Highest single transaction amount for that category on that date.
Avg Amount	Average amount for that date/ category.
Total Amount	Sum of all transaction amounts for that date/ category.
Total Transactions	Number of transactions for that date/ category.
Totals (per Category)	Aggregate Min/ Max/ Avg/ Total Amount and Total Transactions across the selected date range for that category.

Application

Use this report to:

- Monitor volume and value of Teller monetary activity by category and day.
- Identify unusual amount patterns (e.g., very high or very low averages) requiring review.
- Track the mix of transfer directions (checking→checking vs checking→savings vs savings→savings).
- Review Stop Payment activity levels over time for operational or risk analysis.
- Support capacity and process planning for Teller features within SmartApps.

> **Example:** If "Funds Transfer – Checking to Savings" shows a sudden increase in Total Transactions and Total Amount on certain dates, validate whether a campaign, payroll timing, or configuration change drove the surge.

Tips for Users

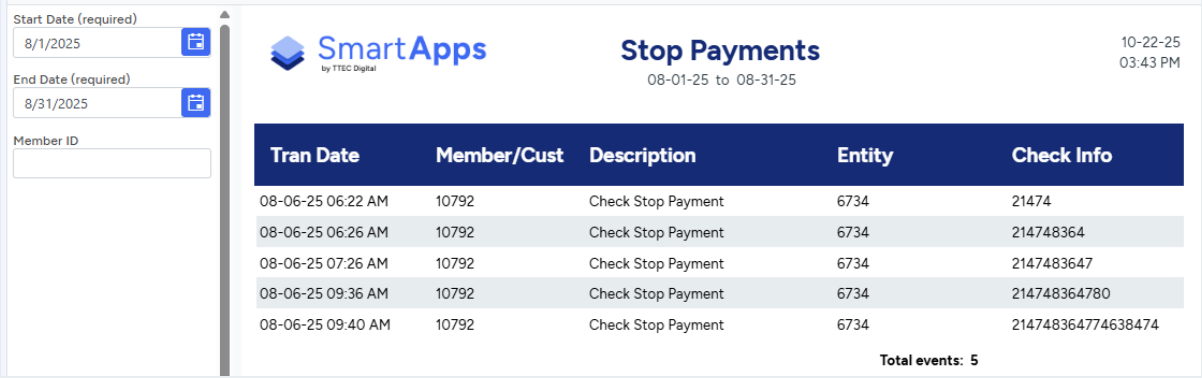
- Compare category totals month-over-month to **spot trend shifts** in member behavior.
- Investigate dates where Min Amount = Max Amount with higher counts; this may indicate **scripted or repeated nominal transactions.**
- Pair with **Confirmation Audit History** to drill from category/ day summaries into individual transaction confirmations when needed.
- If you require per-teller balancing or cash-drawer reconciliation, use your institution's cash management reports; this report is optimized for category activity, not drawer settlement.

Stop Payments

Description

The Stop Payments report captures non-monetary transactions where a member instructed the system to prevent a check from being processed or cleared. Each entry reflects a confirmed stop-payment action initiated through SmartApps and displays the check identifier and associated account/ entity on which the stop was placed. The report shows each request individually and provides a total count of events at the bottom.

This report lists all stop-payment requests submitted through the IVR/ SmartApps channel within the selected date range, including the member, transaction time-stamp, and check reference details.



Key Concepts

- **Stop Payment Event**
  A request to block a check or check series from being honored by the core. These events are marked as completed IVR actions even if the check value is $0.00 (non-cash action).

- **Member Originated**

  Only stop payments initiated by members through the IVR/ SmartApps channel are included.

- **Entity and Check Info**

  The “Entity” identifies the account or routing context within which the stop is applied; “Check Info” identifies the actual check or series affected.

What you will see in the report

Field	Description
Tran Date	Timestamp when the stop payment request was submitted through IVR.
Member or Customer	Member ID of the requester.
Description	Will show “Check Stop Payment” for all entries in this report.
Entity	Account or check-holding context on which the stop is being placed (e.g., share/ loan/ checking identifier).
Check Info	Individual check number or check reference string provided by the member at the time of entry.
Total	Count of all stop-payment transactions processed during the selected period.

Application

Use this report to:

- **Validate** that member-initiated stop payments were successfully captured.
- **Investigate** disputes or member claims related to stopped items.
- **Monitor** volume and frequency of check stop requests over time.

- **Identify** potential abusive or repetitive stop-payment patterns.
- **Provide** event evidence for operational or risk/ audit follow-up.

> **Example:** If a member claims they requested a stop on "check 2147483647," the report provides the submission date and check reference for verification.

Tips for Users

- Cross-reference with **Confirmation Audit History** if additional details or context are required.
- Review repetitive stop requests from the same member to **detect potential misuse** or recurring disputes.
- Use for operational traceability rather than financial balancing (**amount is not shown because stop payment is a non-cash action**).
- Combine with **Monetary Transactions** when evaluating overall check-handling behavior across channels.

Transfers By Destination

Description

The Transfers By Destination report is used to understand where self-service ends and agent assistance begins. Each transfer indicates that the Teller IVR could not, or should not, complete the interaction autonomously. The report organizes these events by the configured call-center destination (e.g., Member Services, Mortgage Queue, Collections) and shows which Teller menu and self-service functions the caller was on when the escalation occurred, along with the reason the transfer was triggered.

This report provides a daily summary of calls that exited the Teller IVR flows and were transferred to a live agent. Transfers are grouped by destination (the call-center department or skill group) and further broken down by the menu or the self-service function the caller was in when the transfer occurred and the reason for the transfer.

> **Note:** When a destination is shown as 'Unassigned', it means no department mapping has been configured yet; the call still reached an agent, but the target department is not labeled in the system.

SmartApps by TTEC Digital

Teller - Transfers By Destination

07-31-25 to 02-07-26

01-22-26
05:04 PM

Member Services

Set Interaction Mode	Reason	Transfer Count
	Entry Timeout - No Response From Caller	1

Unassigned

Account Balances	Reason	Transfer Count
	Customer Request	1

Automation - Agent Transfer 1 / DO NOT MODIFY	Reason	Transfer Count
	Customer Request	5

Caller Authentication	Reason	Transfer Count
	Authentication Failed	12

Check Number Inquiry	Reason	Transfer Count
	Entry Timeout - No Response From Caller	1

Deposit to Deposit transfers	Reason	Transfer Count
	Entry Timeout - No Response From Caller	5

Last Payroll Deposit	Reason	Transfer Count
	Customer Request	1

Mortgage Information and Transaction Menu	Reason	Transfer Count
	Customer Request	3
	Entry Timeout - No Response From Caller	1

Key Concepts

- **Destination(Top Header Row)**

  Represents the call-center department or skill group the caller was routed to (e.g., Member Services). If not configured, it displays **Unassigned**.

- **Source Menu (Second Row)**

  Represents the Teller menu or the self-service function where the caller was when they left IVR (e.g., Mortgage Information and Transaction Menu).

- **Transfer Reasons**

  Identifies why the call was escalated. Common categories include:

  - Authentication Failure
  - Customer Request
  - System Exception or Unable to Process
  - Business Rule Transfers (e.g., collections, mortgage support)
  - No Input

- **Volume Interpretation**

  High transfer counts from a destination indicate that callers frequently require agent assistance at that specific point in the Teller flow.

- **Agent Transfer Event**

  Every row in this report represents a successful hand-off to a live agent—not a transfer to another automated menu.

What you will see in the report

Field	Description
Destination	Call-center department or queue where the call was sent.
Source (Menu Name)	The IVR or self-service menu where the caller was located

Field	Description
	at the moment the transfer occurred. In some cases, this represents a self-service function (for example, Check Account Information) rather than a navigational menu.
Reason	Why the caller left IVR (request, timeout, policy, failure, etc.).
Transfer Count	Number of calls transferred for that reason from that menu or self service functions to that destination.
Total	Total transfers per destination for the date range.

Application

Use this report to:

Fraud & Security Teams

- Identify authentication-related transfer spikes
- Correlate failed authentication transfers with fraud risk patterns

Contact Center & IVR Operations

- Detect self-service friction points
- Optimize IVR flows to reduce unnecessary agent transfers
- Balance automation vs live-agent demand

Business & Experience Teams

- Understand customer behavior within self-service menus
- Improve call containment and customer satisfaction
- Support data-driven IVR redesign initiatives

Tips for Users

- Configure destination mapping to replace **Unassigned** values with real departments for clearer reporting.
- Compare with **Call Flow Analysis** to identify menus and self-service functions with high usage and high transfer rates.
- Investigate repeated **Customer Request** vs. **No Input**- one indicates choice, the other friction.
- Review after IVR wording or routing changes to confirm expected reduction or increase in transfers.
- Use trends over time to distinguish persistent design issues from one-time anomalies.

Activity By Source

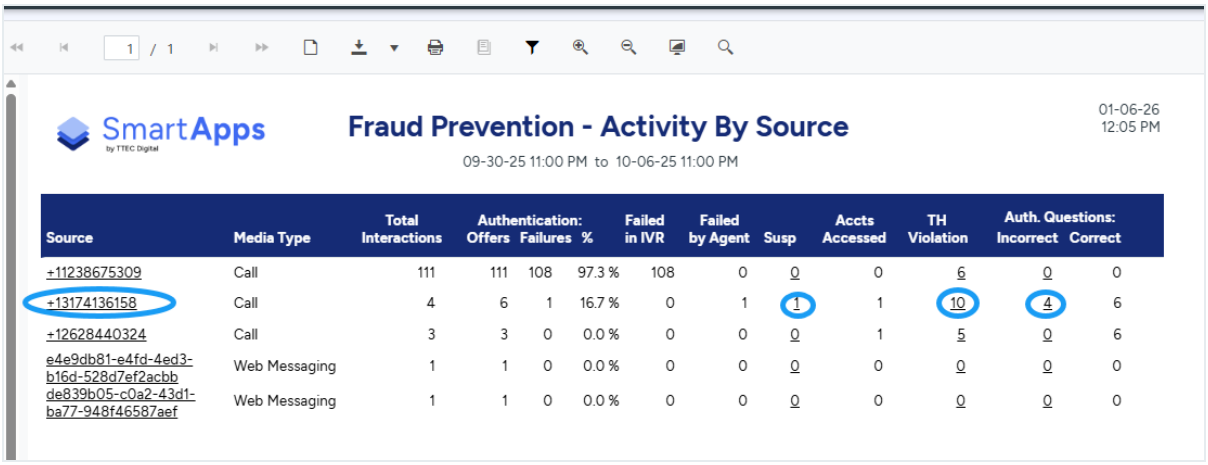
Description

The Activity by Source report summarizes SmartApps activity by the originating source (phone number, email address, or web session ID) for the selected date range. Each row represents one source and shows how often it interacted, how authentication performed, whether account data was accessed, and whether any fraud thresholds were triggered.

The report also includes **drill-down navigation**. Clicking Source ID, Suspicious counts, Threshold Violations, Authentication Question results, or Interaction IDs opens detailed views of the associated interactions, questions, violations, or full interaction records to support deeper analysis.

This report supports both:

- **proactive monitoring** – detecting emerging fraud activity while it is still in progress
- **post-event investigations** – reviewing origins after a confirmed or suspected fraud event



1 / 1

SmartApps

Fraud Prevention - Activity By Source

09-30-25 11:00 PM to 10-06-25 11:00 PM

01-06-26
12:05 PM

Source	Media Type	Total Interactions	Authentication: Offers	Failures	%	Failed in IVR	Failed by Agent	Susp	Accts Accessed	TH Violation	Auth. Questions: Incorrect	Correct
+11238675309	Call	111	111	108	97.3 %	108	0	0	0	6	0	0
+13174136158	Call	4	6	1	16.7 %	0	1	1	1	10	4	6
+12628440324	Call	3	3	0	0.0 %	0	0	0	1	5	0	6
e4e9db81-e4fd-4ed3-b16d-528d7ef2acbb	Web Messaging	1	1	0	0.0 %	0	0	0	0	0	0	0
de839b05-c0a2-43d1-ba77-948f46587aef	Web Messaging	1	1	0	0.0 %	0	0	0	0	0	0	0

Key Concepts

- **Source ID**

  Identifies the origin of the interaction (ANI for calls, session hash for web, email for digital). Used to trace behaviors to a single origin.

- **Authentication Monitoring**

  Shows how often authentication was presented, passed, or failed. High failure rates are an early indicator of potential fraud attempts.

- **Failed in IVR vs. Failed by Agent**

  Separates automatically detected failures from manual failures recorded by agents during live verification.

- **Suspicious Flagging**

  Indicates interactions that agents have flagged as suspicious based on caller behavior, responses, or conversation context.

- **Threshold Violations**

  Indicates that the source triggered predefined fraud-prevention thresholds such as excessive call velocity, repeated authentication failure, or suspicious history rules.

- **Accounts Accessed**

  Indicates whether protected account information was successfully accessed. This is a critical escalation signal indicating heightened fraud risk.

What you will see in the report

Field	Description
Source	Identifier of the entity generating the interaction (phone #, session ID, email).
Media Type	Channel used (Call, Web Messaging, etc.).
Total Interactions	Number of interactions associated with this source dur-

Field	Description
	ing the selected period.
Authentication Offers	Number of times authentication challenges were presented.
Authentication Failures / %	Count and percentage of failed authentication attempts.
Failed in IVR	Authentication failures detected automatically.
Failed by Agent	Authentication failures recorded by an agent.
Suspicious	Number of interactions flagged as suspicious by an agent.
Accounts Accessed	Indicates whether account data was accessed.
TH Violations	Number of fraud-prevention rule violations tied to this source.
Auth Questions: Incorrect / Correct	Counts of incorrect and correct authentication responses.

Drill-Down Navigation

Several fields in the report are interactive. Selecting the underlined value opens supporting detail reports providing deeper investigation capability.

Click the Source ID

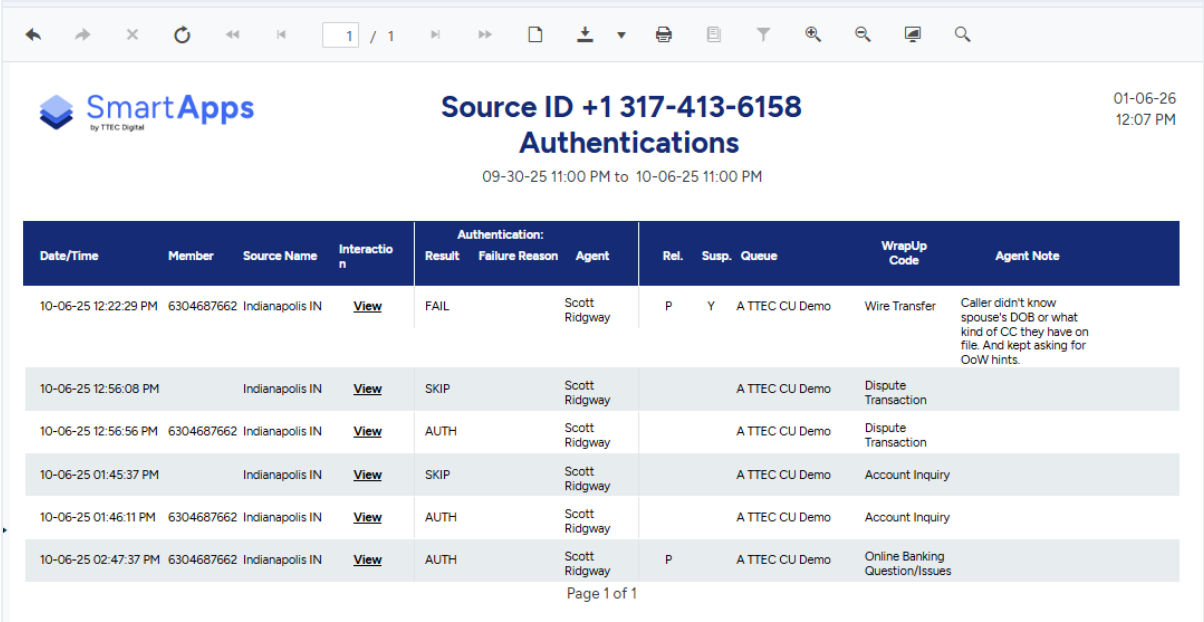
Opens the **Source ID – Authentications** report. This drill-down displays every interaction tied to that source including:

- date and time
- media type
- authentication result (AUTH, FAIL, SKIP)
- failure reason
- handling agent

- queue and wrap-up code
- agent notes

In the S**ource ID – Authentications** drill-down report, the **View** link next to each interaction opens the detailed record within the Genesys platform. Users may be prompted to authenticate based on role permissions.

> **Tip:** Use this view to analyze behavioral patterns and authentication outcomes tied to a specific phone number or device/session.



SmartApps by TTEC Digital

Source ID +1 317-413-6158
Authentications

09-30-25 11:00 PM to 10-06-25 11:00 PM

01-06-26
12:07 PM

Date/Time	Member	Source Name	Interaction	Authentication: Result	Failure Reason	Agent	Rel.	Susp.	Queue	WrapUp Code	Agent Note
10-06-25 12:22:29 PM	6304687662	Indianapolis IN	View	FAIL		Scott Ridgway	P	Y	A TTEC CU Demo	Wire Transfer	Caller didn't know spouse's DOB or what kind of CC they have on file. And kept asking for OoW hints.
10-06-25 12:56:08 PM		Indianapolis IN	View	SKIP		Scott Ridgway			A TTEC CU Demo	Dispute Transaction	
10-06-25 12:56:56 PM	6304687662	Indianapolis IN	View	AUTH		Scott Ridgway			A TTEC CU Demo	Dispute Transaction	
10-06-25 01:45:37 PM		Indianapolis IN	View	SKIP		Scott Ridgway			A TTEC CU Demo	Account Inquiry	
10-06-25 01:46:11 PM	6304687662	Indianapolis IN	View	AUTH		Scott Ridgway			A TTEC CU Demo	Account Inquiry	
10-06-25 02:47:37 PM	6304687662	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Online Banking Question/Issues	

Page 1 of 1

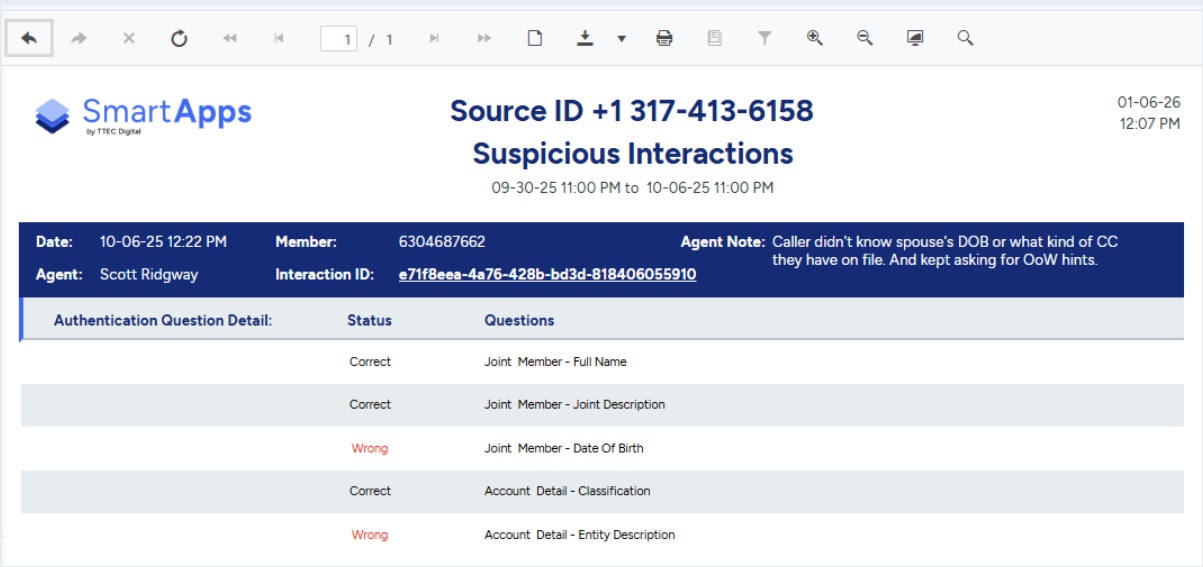
Click the Suspicious Count

Opens the **Source ID – Suspicious Interaction**s report. This report lists agent-flagged suspicious contacts and shows:

- interaction details
- impacted member(s)
- authentication questions asked

- each answer marked correct or incorrect
- agent notes providing the rationale for the suspicious flag

> **Tip:** This report is commonly used for documentation supporting case investigation or account restriction.

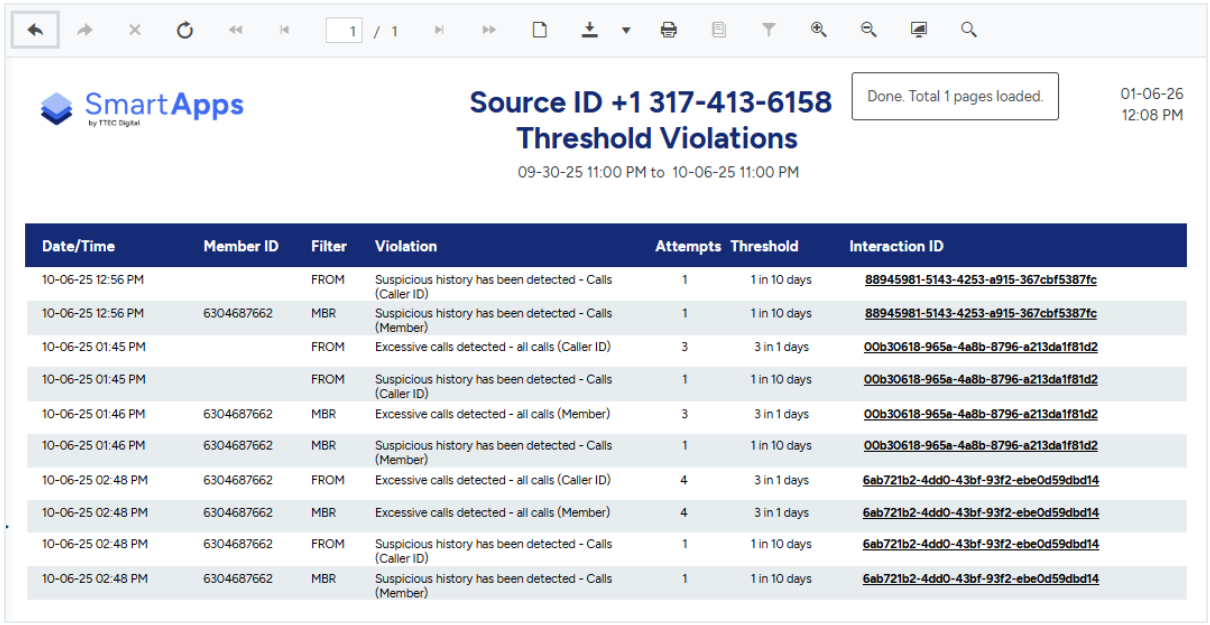


Click Threshold Violations

Opens the **Source ID – Threshold Violations** report. This report details rule triggers including:

- violation type
- attempt count versus configured threshold
- impacted member ID
- associated interaction ID

> **Tip:** Use this view to confirm why a source was classified as high risk and to validate fraud-rule performance.



SmartApps

Source ID +1 317-413-6158
Threshold Violations
09-30-25 11:00 PM to 10-06-25 11:00 PM

Done. Total 1 pages loaded.

01-06-26
12:08 PM

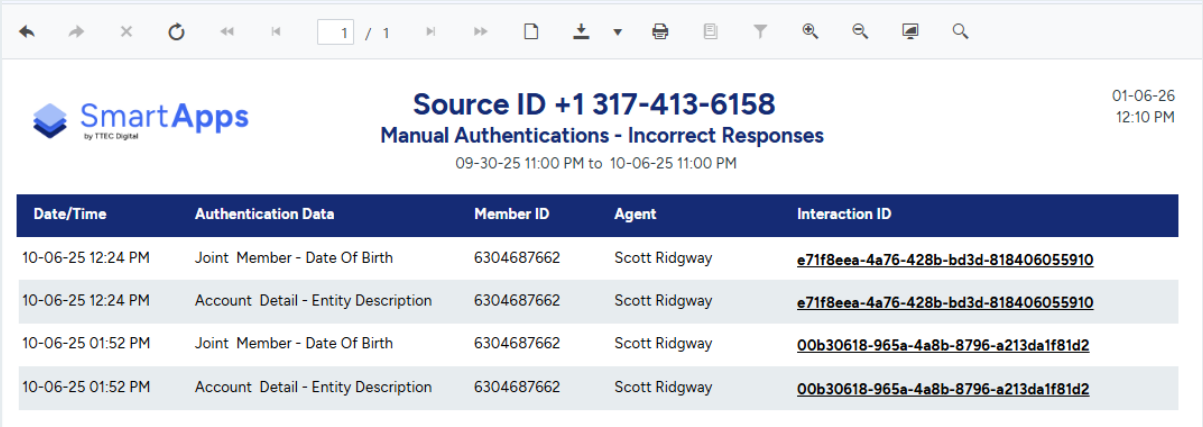
Date/Time	Member ID	Filter	Violation	Attempts	Threshold	Interaction ID
10-06-25 12:56 PM		FROM	Suspicious history has been detected - Calls (Caller ID)	1	1 in 10 days	88945981-5143-4253-a915-367cbf5387fc
10-06-25 12:56 PM	6304687662	MBR	Suspicious history has been detected - Calls (Member)	1	1 in 10 days	88945981-5143-4253-a915-367cbf5387fc
10-06-25 01:45 PM		FROM	Excessive calls detected - all calls (Caller ID)	3	3 in 1 days	00b30618-965a-4a8b-8796-a213da1f81d2
10-06-25 01:45 PM		FROM	Suspicious history has been detected - Calls (Caller ID)	1	1 in 10 days	00b30618-965a-4a8b-8796-a213da1f81d2
10-06-25 01:46 PM	6304687662	MBR	Excessive calls detected - all calls (Member)	3	3 in 1 days	00b30618-965a-4a8b-8796-a213da1f81d2
10-06-25 01:46 PM	6304687662	MBR	Suspicious history has been detected - Calls (Member)	1	1 in 10 days	00b30618-965a-4a8b-8796-a213da1f81d2
10-06-25 02:48 PM	6304687662	FROM	Excessive calls detected - all calls (Caller ID)	4	3 in 1 days	6ab721b2-4dd0-43bf-93f2-ebe0d59dbd14
10-06-25 02:48 PM	6304687662	MBR	Excessive calls detected - all calls (Member)	4	3 in 1 days	6ab721b2-4dd0-43bf-93f2-ebe0d59dbd14
10-06-25 02:48 PM	6304687662	FROM	Suspicious history has been detected - Calls (Caller ID)	1	1 in 10 days	6ab721b2-4dd0-43bf-93f2-ebe0d59dbd14
10-06-25 02:48 PM	6304687662	MBR	Suspicious history has been detected - Calls (Member)	1	1 in 10 days	6ab721b2-4dd0-43bf-93f2-ebe0d59dbd14

Click Incorrect Authentication Questions

Opens the **Manual Authentications – Incorrect Responses** report. This view presents:

- which authentication questions were missed
- member ID affected
- handling agent
- associated interaction ID

> **Tip:** This view is useful for detecting knowledge-based probing, repeated guessing, or stolen-data testing activity.



SmartApps by TTEC Digital

Source ID +1 317-413-6158

Manual Authentications - Incorrect Responses

09-30-25 11:00 PM to 10-06-25 11:00 PM

01-06-26
12:10 PM

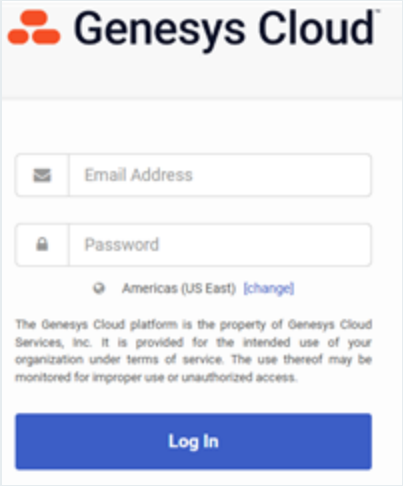
Date/Time	Authentication Data	Member ID	Agent	Interaction ID
10-06-25 12:24 PM	Joint Member - Date Of Birth	6304687662	Scott Ridgway	e71f8eea-4a76-428b-bd3d-818406055910
10-06-25 12:24 PM	Account Detail - Entity Description	6304687662	Scott Ridgway	e71f8eea-4a76-428b-bd3d-818406055910
10-06-25 01:52 PM	Joint Member - Date Of Birth	6304687662	Scott Ridgway	00b30618-965a-4a8b-8796-a213da1f81d2
10-06-25 01:52 PM	Account Detail - Entity Description	6304687662	Scott Ridgway	00b30618-965a-4a8b-8796-a213da1f81d2

Click the Interaction ID

Opens **full interaction detail in the contact platform**. Selecting an **Interaction ID** launches the detailed record in the contact platform (for example, Genesys Cloud). Users may be prompted to authenticate before viewing and includes:

- full call or chat transcript
- audio recording (if enabled)
- IVR path and transfer history
- agent notes and wrap-up codes
- detailed event timeline

> **Tip:** This drill-down provides detail required for fraud case review and compliance documentation.



Application

Use this report to:

- **Fraud & Security Teams**:
    - Identify recurring fraud attempts from the same source.
    - Prioritize high-risk sources with both failure activity and account access.
    - Investigate suspicious or repeat threshold violators.
- **Contact Center Supervisors**:
    - Identify callers escalating authentication challenges to agents.
    - Monitor suspicious tags and agent-identified threats.
    - Correlate authentication problems with call handling outcomes.
- **Business / Operations Admins**:
    - Detect abnormal spikes in originating activity (possible fraud wave).
    - Compare self-service vs. assisted fraud behavior.
    - Validate effectiveness of authentication controls.

Tips for Users

- High failure rates with **no access** typically indicate probing or testing behavior
- High failure rates **with access** require immediate escalation
- Unusual activity concentration from a single source may indicate a broader fraud campaign
- Apply filters (date range, channel, threshold type) for targeted analysis
- Cross-reference this report with **Fraud Investigator** for full interaction-level detail
- Prioritize review of sources with both **threshold violations and suspicious flags**
- Share repeat-offender source IDs for blocking or exclusion list action

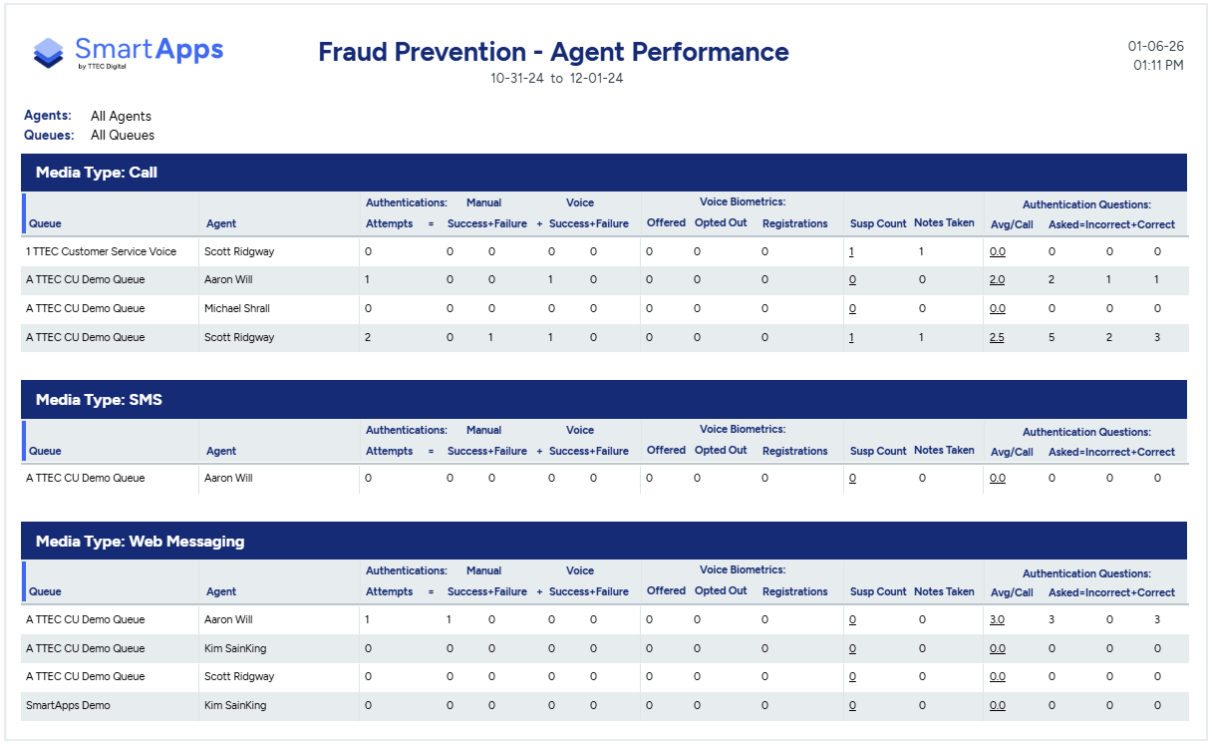
Agent Performance

Description

The Agent Performance report tracks agent behavior specifically in the context of fraud prevention controls — not general call handling. It shows how often agents attempt authentication, how many times they succeed or fail, how consistently they ask identity verification questions, and how frequently they identify and tag interactions as suspicious.

Because fraud attempts often surface during live agent engagement, this report is a primary tool for determining whether agents are **correctly enforcing authentication controls** and **appropriately escalating risky interactions**.

This report evaluates how agents handle fraud-sensitive interactions by measuring authentication activity, suspicious call tagging, and adherence to verification procedures across different media types (Call, SMS, Web Messaging). It supports compliance auditing, fraud investigation, and performance coaching.



SmartApps by TTEC Digital

Fraud Prevention - Agent Performance

10-31-24 to 12-01-24

01-06-26
01:11 PM

Agents: All Agents
Queues: All Queues

Media Type: Call

Queue	Agent	Authentications: Attempts	=	Manual Success+Failure	+	Voice Success+Failure	Voice Biometrics: Offered	Opted Out	Registrations	Susp Count	Notes Taken	Authentication Questions: Avg/Call	Asked=Incorrect+Correct		
1 TTEC Customer Service Voice	Scott Ridgway	0		0	0	0	0	0	0	1	1	0.0	0	0	0
A TTEC CU Demo Queue	Aaron Will	1		0	1	0	0	0	0	0	0	2.0	2	1	1
A TTEC CU Demo Queue	Michael Shrall	0		0	0	0	0	0	0	0	0	0.0	0	0	0
A TTEC CU Demo Queue	Scott Ridgway	2		0	1	0	0	0	0	1	1	2.5	5	2	3

Media Type: SMS

Queue	Agent	Authentications: Attempts	=	Manual Success+Failure	+	Voice Success+Failure	Voice Biometrics: Offered	Opted Out	Registrations	Susp Count	Notes Taken	Authentication Questions: Avg/Call	Asked=Incorrect+Correct		
A TTEC CU Demo Queue	Aaron Will	0		0	0	0	0	0	0	0	0	0.0	0	0	0

Media Type: Web Messaging

Queue	Agent	Authentications: Attempts	=	Manual Success+Failure	+	Voice Success+Failure	Voice Biometrics: Offered	Opted Out	Registrations	Susp Count	Notes Taken	Authentication Questions: Avg/Call	Asked=Incorrect+Correct		
A TTEC CU Demo Queue	Aaron Will	1		1	0	0	0	0	0	0	0	3.0	3	0	3
A TTEC CU Demo Queue	Kim SainKing	0		0	0	0	0	0	0	0	0	0.0	0	0	0
A TTEC CU Demo Queue	Scott Ridgway	0		0	0	0	0	0	0	0	0	0.0	0	0	0
SmartApps Demo	Kim SainKing	0		0	0	0	0	0	0	0	0	0.0	0	0	0

Key Concepts

- **Media Type**

  Channel used for interaction (Call, SMS, Web Messaging, etc.). Options vary by deployment.

- **Queue Context**

  Each interaction is associated with a queue (for example: Member Care, Loans, Cards), allowing comparison across business units or departments.

- **Authentication Attempts**

  Indicates how many times an agent initiated a verification process.

- **Authentication Success vs. Failure**

  Indicates whether authentication was successfully completed or failed while the interaction was handled by the agent.

- **Suspicious Count (Agent Driven)**

  Number of interactions where the agent manually flagged the call as suspicious.

- **Notes Taken**

  Indicates whether the agent documented the interaction. Notes are critical for audit support and investigation.

- **Average Questions Asked per Call**

  Shows whether agents are consistently asking the expected number of authentication questions.

- **Auth Questions Breakdown**

  Tracks the number of correct and incorrect responses to authentication questions.

What you will see in the report

Field	Description
Media Type	Interaction channel (Call, SMS, Web Messaging).
Queue	Department or skill group handling the interaction.
Agent	Specific user handling the fraud-monitored interaction.
Attempts	Count of authentication attempts initiated by agent.
Success / Failure	Authentication outcome counts.
Susp Count	Number of interactions the agent flagged as suspicious.
Notes Taken	Whether notes were documented on the call.
Avg Quest Asked / Call	Average number of authentication questions asked.
Auth Questions: Asked / Incorrect / Correct	Detailed breakdown of authentication response performance.

Drill-Down Navigation

Some values in the report are interactive and open deeper detail to support investigation and coaching.

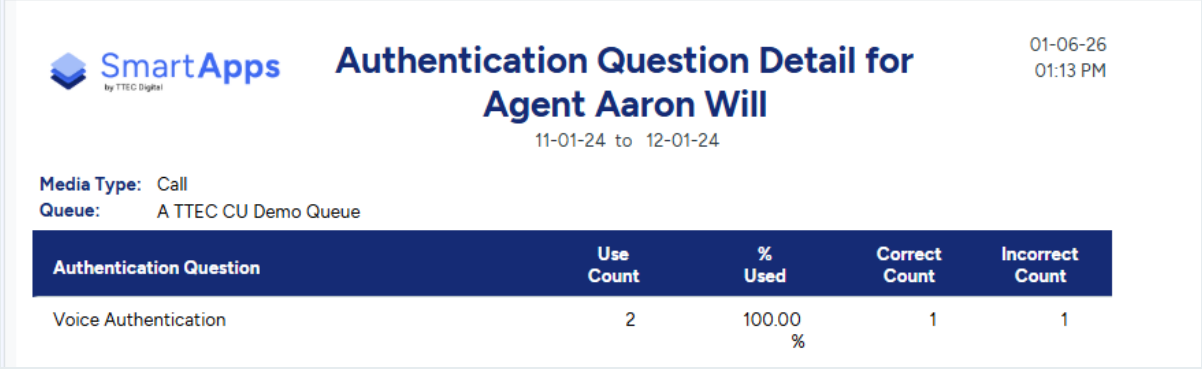
Click Avg/Call under Authentication Questions

Opens Authentication Question Detail for Agent. This drill-down report shows:

- which authentication questions were used
- how often each question was asked
- percentage usage by question type
- correct response count
- incorrect response count

This allows supervisors and fraud teams to determine:

- whether required questions are actually being asked
- whether an agent favors certain questions over others
- whether incorrect responses correlate with suspicious tagging
- if additional coaching is required on verification process execution



SmartApps by TTEC Digital

Authentication Question Detail for Agent Aaron Will

11-01-24 to 12-01-24

01-06-26
01:13 PM

Media Type: Call
Queue: A TTEC CU Demo Queue

Authentication Question	Use Count	% Used	Correct Count	Incorrect Count
Voice Authentication	2	100.00 %	1	1

Application

Use this report to:

- Fraud & Security Teams:
    - **Identify** agents who correctly detect and escalate fraud attempts.
    - **Focus** on agents who never flag calls despite high-risk queues.
    - **Use** as evidence in forensic investigations.
- Contact Center Supervisors:
    - **Verify** agents follow authentication policy consistently.
    - **Identify** training needs and coaching opportunities.
    - **Detect** agents who shortcut verification under workload pressure.
- Business / Compliance:
    - **Validate** internal controls are functioning in live operations.
    - **Compare** performance across branches / queues / channels.
    - **Support** regulatory and audit documentation requirements.

Example Use Case

During a monthly review of the **Agent Performance report**, a supervisor notices that agent **Aaron Will** in the A TTEC CU Demo Queue shows:

- multiple authentication attempts
- authentication questions asked on several calls
- one or more **suspicious tags**
- non-zero incorrect authentication responses

The supervisor drills into the **Avg/Call** value for Aaron Will and opens the **Authentication Question Detail** for Agent report. The detail shows:

- authentication question used: **Voice Authentication**
- use count: 2
- correct responses: 1
- incorrect responses: 1

Interpretation

From the data, the supervisor concludes:

- the agent is consistently attempting authentication
- incorrect answers are being captured and tracked
- the agent is not bypassing identity-verification procedures
- authentication failures and suspicious tagging align

This suggests:

- the agent followed authentication policy
- the agent appropriately challenged the caller
- the incorrect responses may indicate potential account takeover attempts

Action Taken

- fraud operations is notified for pattern review on affected interactions
- interaction records are reviewed in Genesys (via “View” links) to listen to calls
- the agent receives positive feedback for properly executing authentication steps

If multiple incorrect answers were present without suspicious tags, the review outcome would shift to coaching instead of commendation.

Tips for Users

- **Zero suspicious tags in a high-risk queue** = **review required**.
- **High authentication attempts** + **high failure rate** + **no suspicious tags** → **possible agent oversight**.
- **Low average questions per call** = **policy non-compliance**.
- Cross-check this report with **Fraud Prevention – Activity By Source** to link agent behavior to source risk.
- Filter by **Media Type** to compare voice vs messaging behavior.
- Run monthly as part of required fraud control audits or as required.

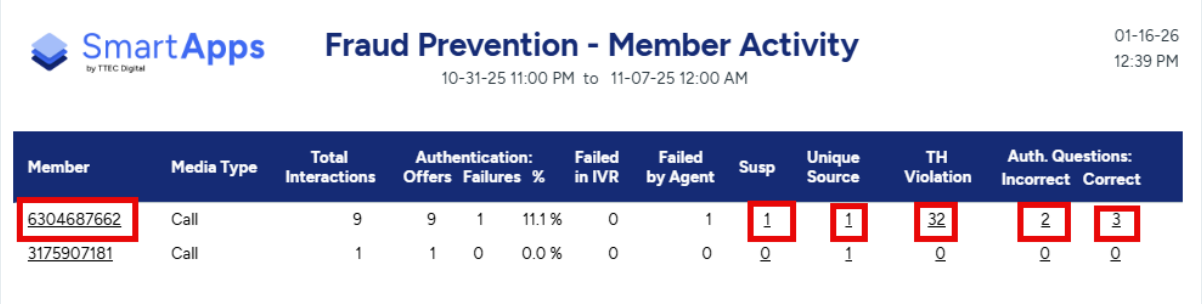
Member Activity

Description

The **Member Activity Report** shows fraud-relevant interaction history grouped by Member ID, across all monitored channels. It highlights **authentication behavior**, **suspicious flags**, **unique interaction sources**, and **threshold violations** tied to a specific member identity.

This report helps identify members with repeated failed authentications, unusual activity patterns, or potential fraud risks by linking authentication outcomes to member accounts and interaction sources.

Because data is grouped by Member ID, the report enables precise investigation of individual member behavior across voice and digital channels, supporting fraud investigation, compliance review, and case documentation.



SmartApps by TTEC Digital

Fraud Prevention - Member Activity

10-31-25 11:00 PM to 11-07-25 12:00 AM

01-16-26
12:39 PM

Member	Media Type	Total Interactions	Authentication: Offers	Failures	%	Failed in IVR	Failed by Agent	Susp	Unique Source	TH Violation	Auth. Questions: Incorrect	Correct
6304687662	Call	9	9	1	11.1 %	0	1	1	1	32	2	3
3175907181	Call	1	1	0	0.0 %	0	0	0	1	0	0	0

Key Concepts

- **Media Type**

  The channel through which the interaction occurred (Call, SMS, Web Messaging, etc.).

- **Authentication Offers**

  Total number of times authentication was presented to the member during interactions.

- **Authentication Failures in %**

  Count and percentage of unsuccessful authentication attempts.

- **Suspicious**

  Count of interactions flagged as suspicious by an agent.

- **Unique Source Count**

  Unique identifiers (phone numbers, messaging IDs) associated with the member's interactions.

- **Threshold Violations (TH)**

  Number of threshold triggers (e.g., excessive contact attempts) related to the member.

- **Authentication Questions – Incorrect or Correct**

  Count of security questions answered incorrectly or correctly during authentication.

What you will see in the report

Field	Description
Member	The account number or identifier of the member.
Media Type	Type of communication (e.g., Call, Web Messaging).
Total Interactions	Total number of member interactions within the selected time frame.
Authentication Offers	Total number of times authentication was required.
Failures %	Number and percentage of failed authentication attempts.

Field	Description
Failed in IVR/ Failed by Agent	Breakdown of automated vs agent-detected failures.
Suspicious	Number of interactions manually marked as suspicious.
Unique Source	Unique interaction source (e.g., phone number, messaging ID).
TH Violation	Number of fraud threshold triggers.
Auth. Questions: Incorrect / Correct	Breakdown of member responses to challenge questions.

Drill-Down Navigation

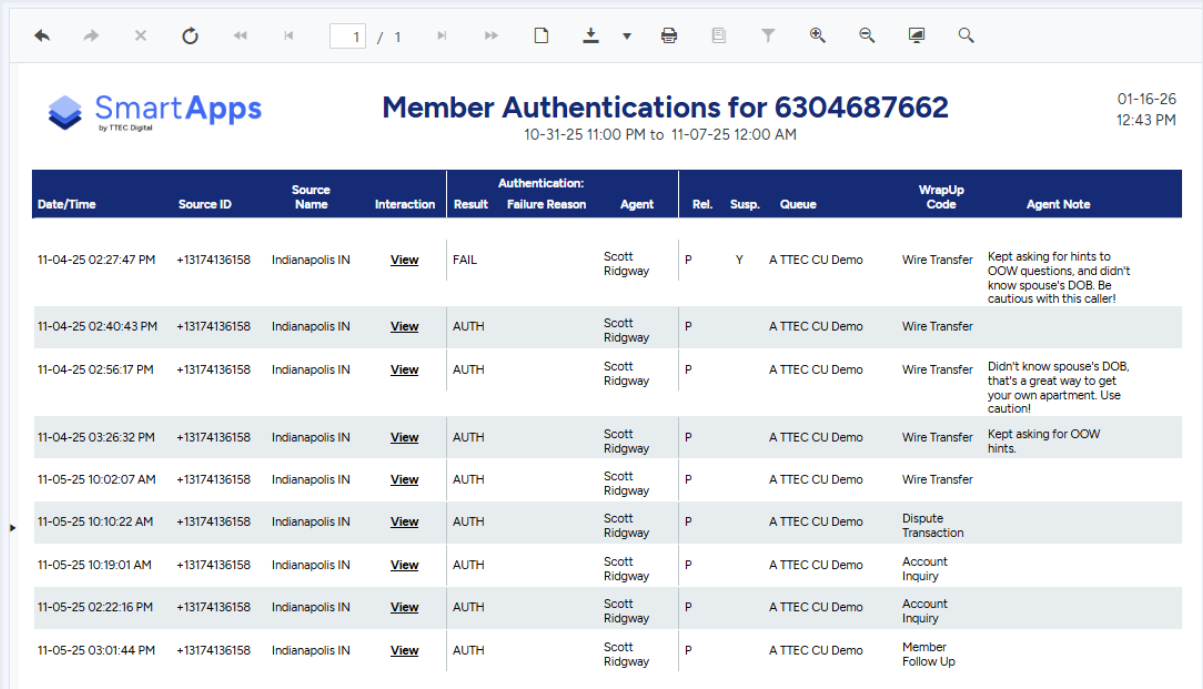
Several values in the Member Activity report are clickable. Selecting a value opens a supporting report that provides deeper investigative context.

Click the Member ID

Opens Member Authentications report. This drill down report lists all interactions associated with the selected member, and includes:

- date and time
- source ID and location
- authentication result (AUTH, FAIL)
- agent handling the interaction
- queue and wrap-up code
- agent notes

> **Tip:** This view is used to review the member's full authentication history across channels.



SmartApps

Member Authentications for 6304687662

10-31-25 11:00 PM to 11-07-25 12:00 AM

01-16-26
12:43 PM

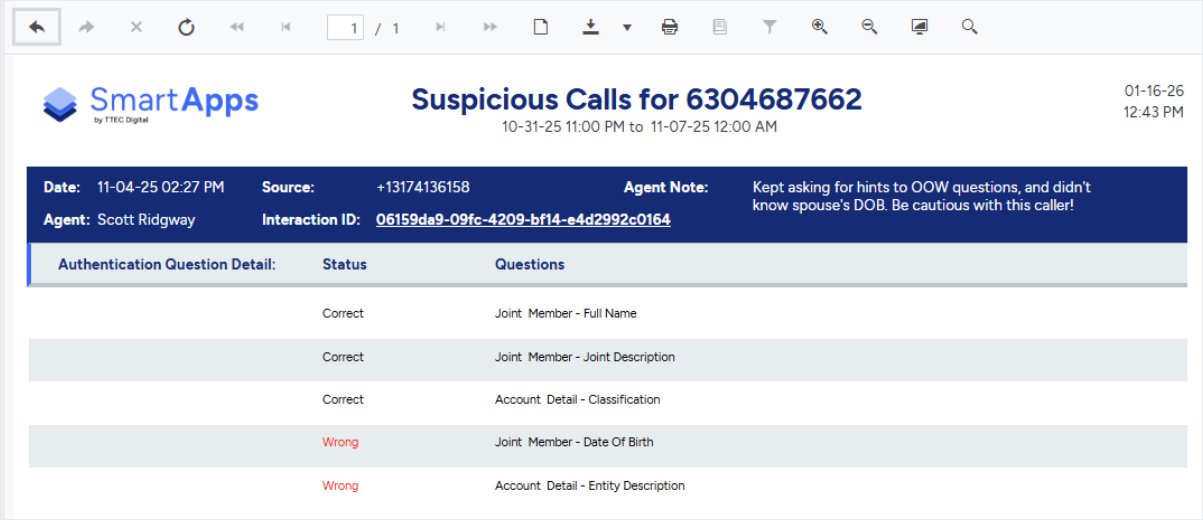
Date/Time	Source ID	Source Name	Interaction	Authentication: Result	Failure Reason	Agent	Rel.	Susp.	Queue	WrapUp Code	Agent Note
11-04-25 02:27:47 PM	+13174136158	Indianapolis IN	View	FAIL		Scott Ridgway	P	Y	A TTEC CU Demo	Wire Transfer	Kept asking for hints to OOW questions, and didn't know spouse's DOB. Be cautious with this caller!
11-04-25 02:40:43 PM	+13174136158	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Wire Transfer	
11-04-25 02:56:17 PM	+13174136158	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Wire Transfer	Didn't know spouse's DOB, that's a great way to get your own apartment. Use caution!
11-04-25 03:26:32 PM	+13174136158	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Wire Transfer	Kept asking for OOW hints.
11-05-25 10:02:07 AM	+13174136158	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Wire Transfer	
11-05-25 10:10:22 AM	+13174136158	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Dispute Transaction	
11-05-25 10:19:01 AM	+13174136158	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Account Inquiry	
11-05-25 02:22:16 PM	+13174136158	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Account Inquiry	
11-05-25 03:01:44 PM	+13174136158	Indianapolis IN	View	AUTH		Scott Ridgway	P		A TTEC CU Demo	Member Follow Up	

Click the Suspicious count

Opens Suspicious Calls for Member. This drill-down shows:

- specific suspicious interaction details
- authentication questions asked
- which responses were correct or wrong
- agent notes explaining the suspicious behavior

> **Tip:** This report is commonly used for fraud case documentation and escalation.

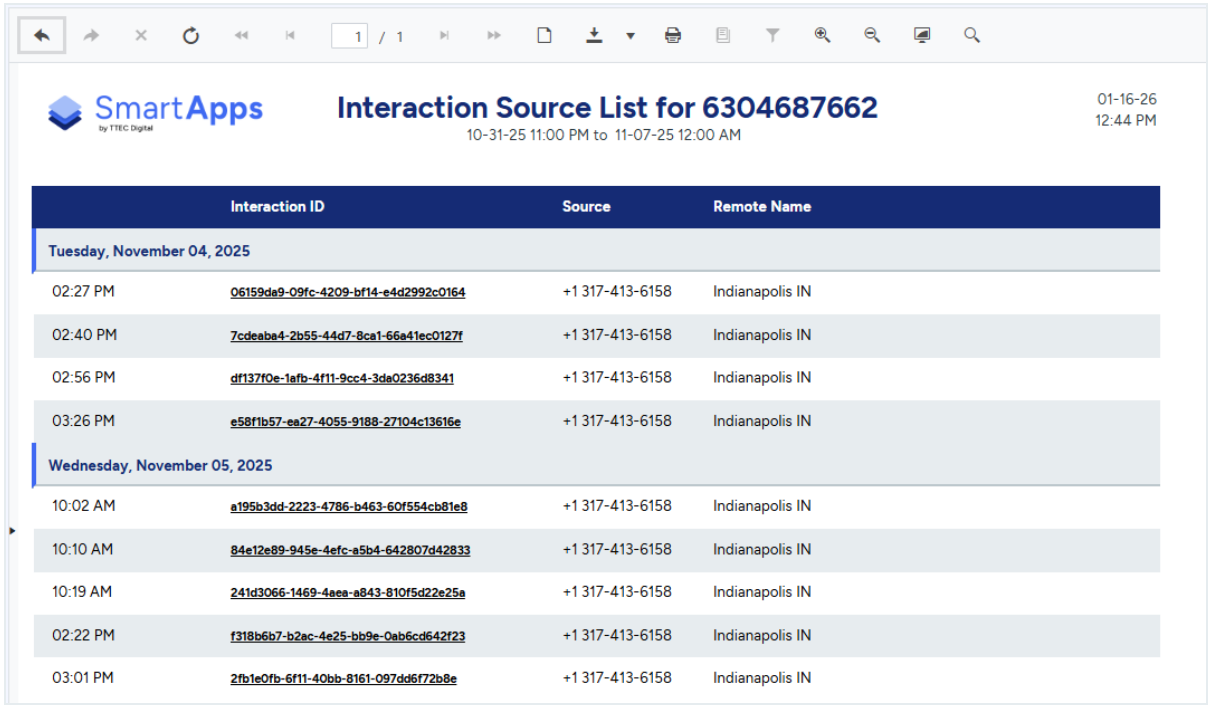


Click the Unique Source count

Opens Interaction Source List for Member. This report displays:

- each interaction ID
- associated source (phone number or messaging ID)
- remote location or source name
- date grouping by interaction day

> **Tip:** This allows investigators to identify reuse of the same source or multiple sources contacting the same member.



SmartApps

Interaction Source List for 6304687662

10-31-25 11:00 PM to 11-07-25 12:00 AM

01-16-26
12:44 PM

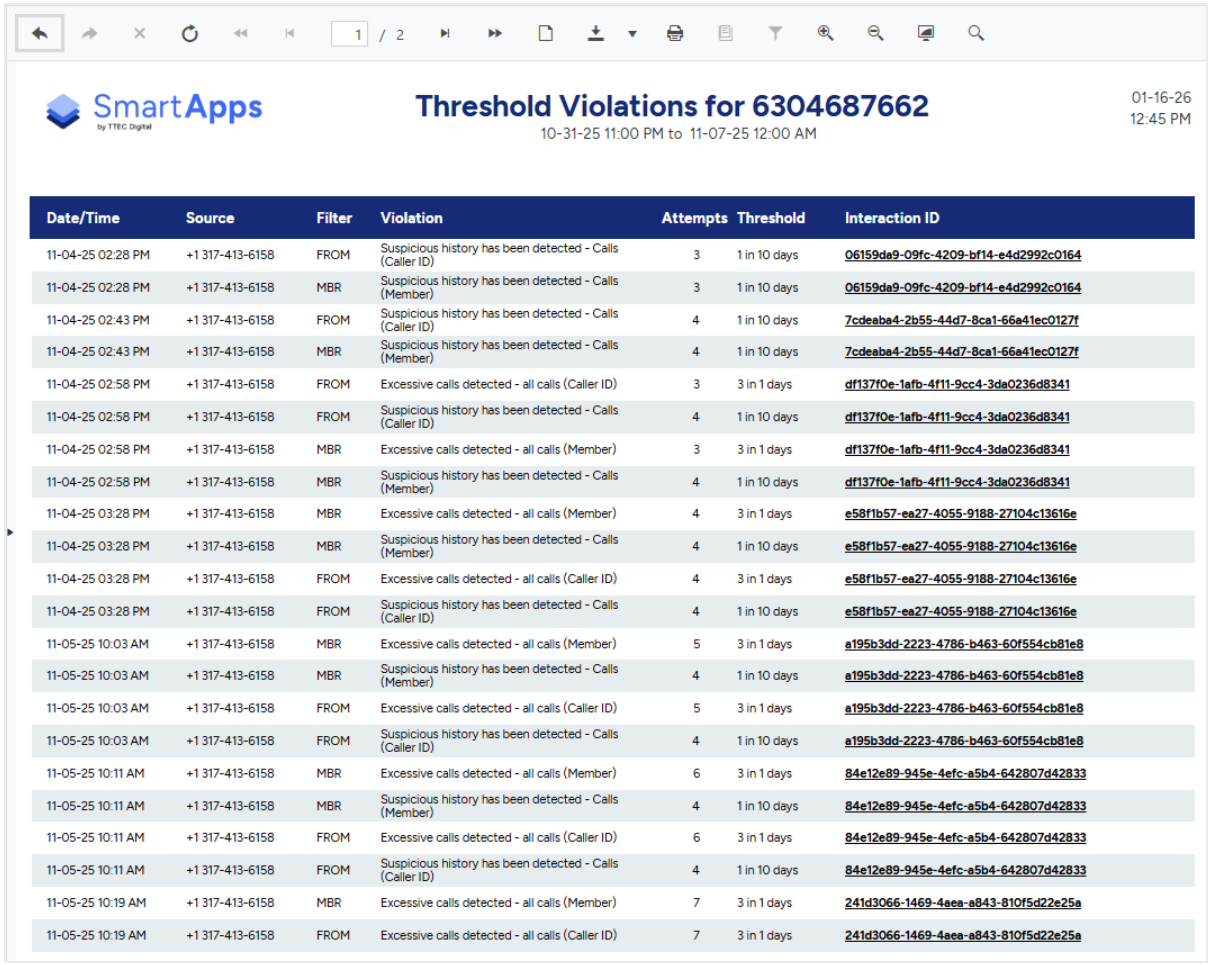
	Interaction ID	Source	Remote Name
Tuesday, November 04, 2025			
02:27 PM	06159da9-09fc-4209-bf14-e4d2992c0164	+1 317-413-6158	Indianapolis IN
02:40 PM	7cdeaba4-2b55-44d7-8ca1-66a41ec0127f	+1 317-413-6158	Indianapolis IN
02:56 PM	df137f0e-1afb-4f11-9cc4-3da0236d8341	+1 317-413-6158	Indianapolis IN
03:26 PM	e58f1b57-ea27-4055-9188-27104c13616e	+1 317-413-6158	Indianapolis IN
Wednesday, November 05, 2025			
10:02 AM	a195b3dd-2223-4786-b463-60f554cb81e8	+1 317-413-6158	Indianapolis IN
10:10 AM	84e12e89-945e-4efc-a5b4-642807d42833	+1 317-413-6158	Indianapolis IN
10:19 AM	241d3066-1469-4aea-a843-810f5d22e25a	+1 317-413-6158	Indianapolis IN
02:22 PM	f318b6b7-b2ac-4e25-bb9e-0ab6cd642f23	+1 317-413-6158	Indianapolis IN
03:01 PM	2fb1e0fb-6f11-40bb-8161-097dd6f72b8e	+1 317-413-6158	Indianapolis IN

Click TH Violations

Opens Threshold Violations for Member. This report lists each triggered fraud-prevention rule, including:

- violation type (excessive calls, suspicious history, etc.)
- attempt count versus threshold definition
- filter context (Caller ID vs Member-based)
- interaction ID tied to the violation

> **Tip:** This view explains why and how fraud rules were triggered for the member.



SmartApps by TTEC Digital

Threshold Violations for 6304687662

10-31-25 11:00 PM to 11-07-25 12:00 AM

01-16-26
12:45 PM

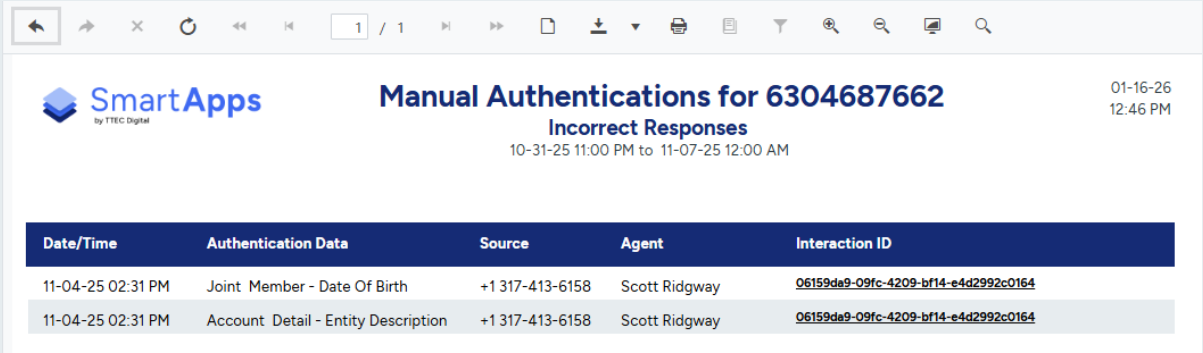
Date/Time	Source	Filter	Violation	Attempts	Threshold	Interaction ID
11-04-25 02:28 PM	+1 317-413-6158	FROM	Suspicious history has been detected - Calls (Caller ID)	3	1 in 10 days	06159da9-09fc-4209-bf14-e4d2992c0164
11-04-25 02:28 PM	+1 317-413-6158	MBR	Suspicious history has been detected - Calls (Member)	3	1 in 10 days	06159da9-09fc-4209-bf14-e4d2992c0164
11-04-25 02:43 PM	+1 317-413-6158	FROM	Suspicious history has been detected - Calls (Caller ID)	4	1 in 10 days	7cdeaba4-2b55-44d7-8ca1-66a41ec0127f
11-04-25 02:43 PM	+1 317-413-6158	MBR	Suspicious history has been detected - Calls (Member)	4	1 in 10 days	7cdeaba4-2b55-44d7-8ca1-66a41ec0127f
11-04-25 02:58 PM	+1 317-413-6158	FROM	Excessive calls detected - all calls (Caller ID)	3	3 in 1 days	df137f0e-1afb-4f11-9cc4-3da0236d8341
11-04-25 02:58 PM	+1 317-413-6158	FROM	Suspicious history has been detected - Calls (Caller ID)	4	1 in 10 days	df137f0e-1afb-4f11-9cc4-3da0236d8341
11-04-25 02:58 PM	+1 317-413-6158	MBR	Excessive calls detected - all calls (Member)	3	3 in 1 days	df137f0e-1afb-4f11-9cc4-3da0236d8341
11-04-25 02:58 PM	+1 317-413-6158	MBR	Suspicious history has been detected - Calls (Member)	4	1 in 10 days	df137f0e-1afb-4f11-9cc4-3da0236d8341
11-04-25 03:28 PM	+1 317-413-6158	MBR	Excessive calls detected - all calls (Member)	4	3 in 1 days	e58f1b57-ea27-4055-9188-27104c13616e
11-04-25 03:28 PM	+1 317-413-6158	MBR	Suspicious history has been detected - Calls (Member)	4	1 in 10 days	e58f1b57-ea27-4055-9188-27104c13616e
11-04-25 03:28 PM	+1 317-413-6158	FROM	Excessive calls detected - all calls (Caller ID)	4	3 in 1 days	e58f1b57-ea27-4055-9188-27104c13616e
11-04-25 03:28 PM	+1 317-413-6158	FROM	Suspicious history has been detected - Calls (Caller ID)	4	1 in 10 days	e58f1b57-ea27-4055-9188-27104c13616e
11-05-25 10:03 AM	+1 317-413-6158	MBR	Excessive calls detected - all calls (Member)	5	3 in 1 days	a195b3dd-2223-4786-b463-60f554cb81e8
11-05-25 10:03 AM	+1 317-413-6158	MBR	Suspicious history has been detected - Calls (Member)	4	1 in 10 days	a195b3dd-2223-4786-b463-60f554cb81e8
11-05-25 10:03 AM	+1 317-413-6158	FROM	Excessive calls detected - all calls (Caller ID)	5	3 in 1 days	a195b3dd-2223-4786-b463-60f554cb81e8
11-05-25 10:03 AM	+1 317-413-6158	FROM	Suspicious history has been detected - Calls (Caller ID)	4	1 in 10 days	a195b3dd-2223-4786-b463-60f554cb81e8
11-05-25 10:11 AM	+1 317-413-6158	MBR	Excessive calls detected - all calls (Member)	6	3 in 1 days	84e12e89-945e-4efc-a5b4-642807d42833
11-05-25 10:11 AM	+1 317-413-6158	MBR	Suspicious history has been detected - Calls (Member)	4	1 in 10 days	84e12e89-945e-4efc-a5b4-642807d42833
11-05-25 10:11 AM	+1 317-413-6158	FROM	Excessive calls detected - all calls (Caller ID)	6	3 in 1 days	84e12e89-945e-4efc-a5b4-642807d42833
11-05-25 10:11 AM	+1 317-413-6158	FROM	Suspicious history has been detected - Calls (Caller ID)	4	1 in 10 days	84e12e89-945e-4efc-a5b4-642807d42833
11-05-25 10:19 AM	+1 317-413-6158	MBR	Excessive calls detected - all calls (Member)	7	3 in 1 days	241d3066-1469-4aea-a843-810f5d22e25a
11-05-25 10:19 AM	+1 317-413-6158	FROM	Excessive calls detected - all calls (Caller ID)	7	3 in 1 days	241d3066-1469-4aea-a843-810f5d22e25a

Click Auth Questions – Incorrect

Opens Manual Authentications – Incorrect Responses. This report shows:

- authentication question failed
- source used
- handling agent
- associated interaction ID

> **Tip:** This drill-down helps identify knowledge-based authentication probing or repeated guessing behavior.



SmartApps by TTEC Digital

Manual Authentications for 6304687662

Incorrect Responses

10-31-25 11:00 PM to 11-07-25 12:00 AM

01-16-26
12:46 PM

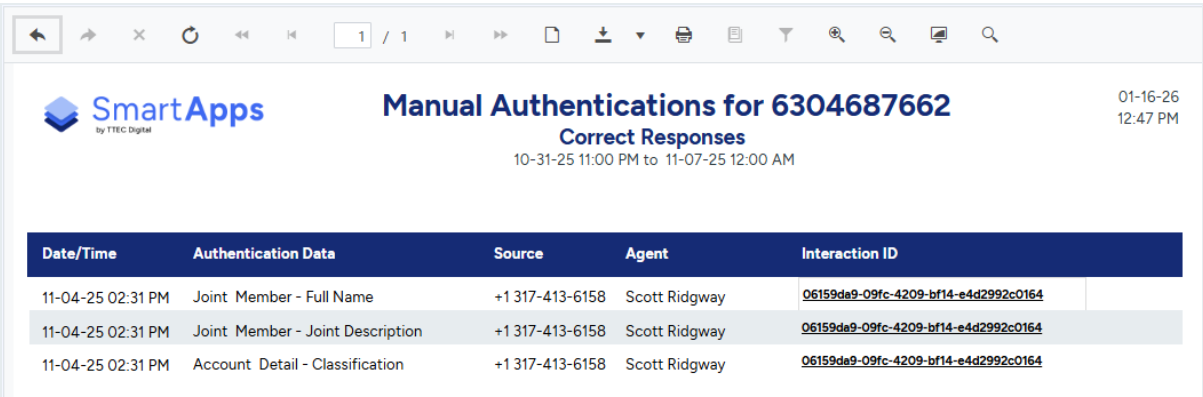
Date/Time	Authentication Data	Source	Agent	Interaction ID
11-04-25 02:31 PM	Joint Member - Date Of Birth	+1 317-413-6158	Scott Ridgway	06159da9-09fc-4209-bf14-e4d2992c0164
11-04-25 02:31 PM	Account Detail - Entity Description	+1 317-413-6158	Scott Ridgway	06159da9-09fc-4209-bf14-e4d2992c0164

Click Auth Questions – Correct

Opens Manual Authentications – Correct Responses. This report lists:

- authentication questions answered correctly
- source ID
- handling agent
- interaction ID

> **Tip:** This allows reviewers to validate that authentication was legitimately passed during certain interactions.



SmartApps by TTEC Digital

Manual Authentications for 6304687662

Correct Responses

10-31-25 11:00 PM to 11-07-25 12:00 AM

01-16-26
12:47 PM

Date/Time	Authentication Data	Source	Agent	Interaction ID
11-04-25 02:31 PM	Joint Member - Full Name	+1 317-413-6158	Scott Ridgway	06159da9-09fc-4209-bf14-e4d2992c0164
11-04-25 02:31 PM	Joint Member - Joint Description	+1 317-413-6158	Scott Ridgway	06159da9-09fc-4209-bf14-e4d2992c0164
11-04-25 02:31 PM	Account Detail - Classification	+1 317-413-6158	Scott Ridgway	06159da9-09fc-4209-bf14-e4d2992c0164

> **Example:** A credit union investigator reviews the Member Activity report for Member 6304687662 after multiple fraud alerts.

Observations

- 9 total call interactions
- 1 suspicious interaction
- 1 unique source repeatedly contacting the member
- 32 threshold violations, primarily related to call frequency
- 2 incorrect and 3 correct authentication question responses

Drill-Down Findings

- Member Authentications show repeated calls from the same phone number
- Suspicious Calls reveal incorrect answers to Date of Birth and Entity Description questions
- Interaction Source List confirms reuse of the same source
- Threshold Violations show excessive call and suspicious-history triggers
- Manual Authentication detail confirms failed and passed challenge questions

Interpretation

The pattern suggests:

- persistent contact from a single source
- knowledge gaps during authentication
- behavior consistent with potential social-engineering or account-takeover attempts

Outcome

- the case is escalated to Fraud Operations
- interaction recordings are reviewed in Genesys
- the member account is monitored for further activity

Application

Use this report to:

- Track **authentication and fraud patterns** for a specific member.
- Detect **repeated failed authentications** or **threshold triggers** that may indicate fraud.
- Correlate authentication failures to **specific channels or sources** (e.g., same phone number, repeated call attempts).
- Review member activity following a **fraud alert or suspicious incident**.
- Provide supporting evidence during **fraud investigations** or compliance audits.

Tips for Users

- Use **Member ID filters** to isolate individual member patterns.
- Pay close attention to **threshold violations** and **suspicious flags** — repeated triggers may indicate attempted fraud.
- Compare this report with**Fraud Prevention – Activity by Source** to trace where the interaction originated.
- If multiple **media types** show abnormal activity, coordinate with fraud prevention teams for cross-channel analysis.
- Schedule **weekly reviews** of members with high failure percentages or repeated suspicious flags.

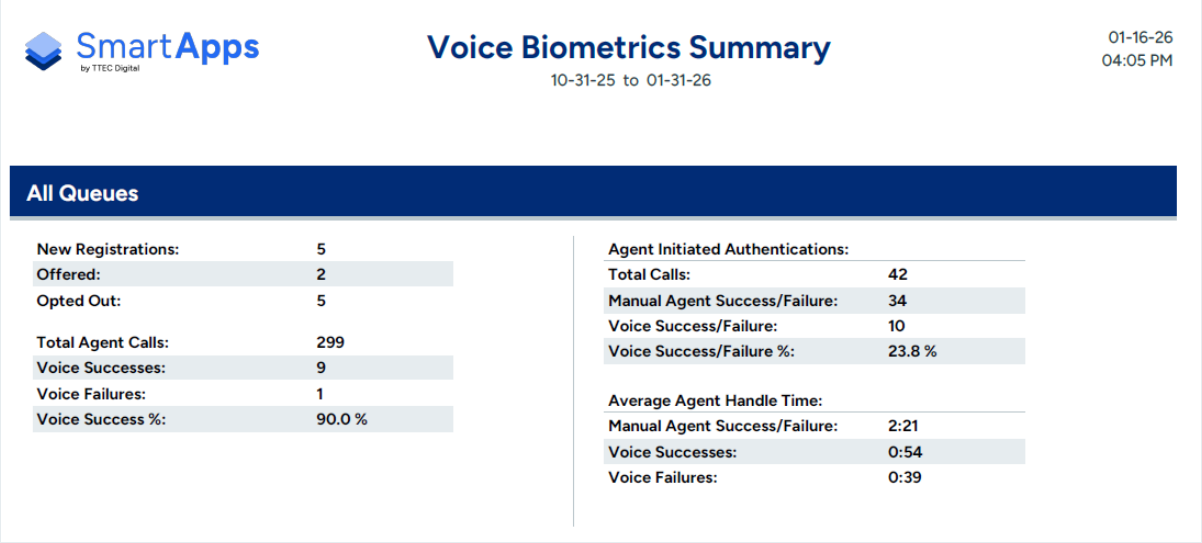
Voice Biometric Summary

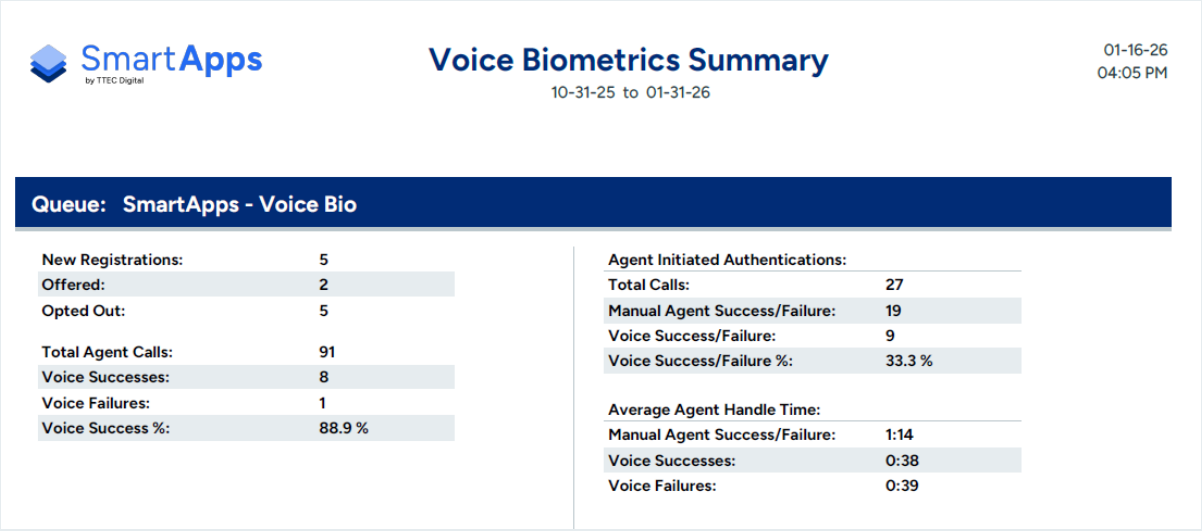
Description

The Voice Biometrics Summary report provides a high-level view of voice biometric authentication activity across queues and agents during the selected date range. It summarizes enrollment activity, voice authentication performance, agent-initiated usage, and success and failure outcomes.

This report is used to evaluate adoption, effectiveness, and operational performance of voice biometrics as a fraud-prevention control. It helps organizations understand where voice biometrics are being offered, how often members opt out, how frequently voice authentication succeeds or fails, and how agents are using voice authentication in live interactions.

Because voice biometrics is a passive authentication mechanism, this report is commonly used for **fraud control validation**, **operational monitoring**, and **compliance reporting**, rather than individual case investigation.





SmartApps by TTEC Digital

Voice Biometrics Summary

10-31-25 to 01-31-26

01-16-26
04:05 PM

Queue: SmartApps - Voice Bio

New Registrations:	5
Offered:	2
Opted Out:	5
Total Agent Calls:	91
Voice Successes:	8
Voice Failures:	1
Voice Success %:	88.9 %

Agent Initiated Authentications:	
Total Calls:	27
Manual Agent Success/Failure:	19
Voice Success/Failure:	9
Voice Success/Failure %:	33.3 %

Average Agent Handle Time:	
Manual Agent Success/Failure:	1:14
Voice Successes:	0:38
Voice Failures:	0:39

Key Concepts

- **New Registrations**

  Number of members newly enrolled in voice biometrics during the period.

- **Offered**

  Number of times voice biometrics enrollment or authentication was offered to callers.

- **Opted Out**

  Number of callers who declined voice biometrics when offered.

- **Voice Successes / Failures**

  Counts of successful and failed voice biometric authentication attempts.

- **Voice Success / Failure %**

  Percentage of successful voice biometric authentications compared to total attempts.

- **Agent-Initiated Authentications**

  Number of times agents manually initiated authentication (non-biometric) during interactions.

- **Manual Agent Success / Failure**

  Outcomes of agent-initiated authentication attempts, including time spent.

- **Total Agent Calls**

  Total number of calls handled by agents in the queue.

- **Average Agent Handle Time**

  Average duration of calls where authentication occurred, segmented by success or failure.

What you will see in the report

Field	Description
Queue	Queue or department handling the interaction.
New Registrations	Number of new voice biometric enrollments.
Offered	Number of voice biometric offers made.
Opted Out	Number of callers who declined enrollment or use.
Voice Successes	Successful voice biometric authentications.
Voice Failures	Failed voice biometric authentications.
Voice Success / Failure	Total biometric attempts.
Voice Success / Failure %	Percentage of successful authentications.
Total Agent Calls	Total calls handled by the queue.
Agent Initiated Authentic-ations	Number of manual authentications initiated by agents.
Manual Agent Success / Failure	Outcome and time spent on manual authentication.
Voice Success %	Percentage of successful voice authentications relative to total voice attempts.

Application

Fraud & Security Teams

- Validate effectiveness of voice biometrics as a fraud-prevention control
- Identify queues with high failure rates requiring tuning or investigation
- Monitor adoption and opt-out rates

Contact Center Operations

- Measure agent reliance on manual authentication versus voice biometrics
- Compare handle time between biometric and manual authentication flows
- Identify queues where voice biometrics is underutilized

Compliance & Audit

- Provide evidence of layered authentication controls
- Demonstrate consistent application of biometric verification
- Support regulatory and internal audit requirements

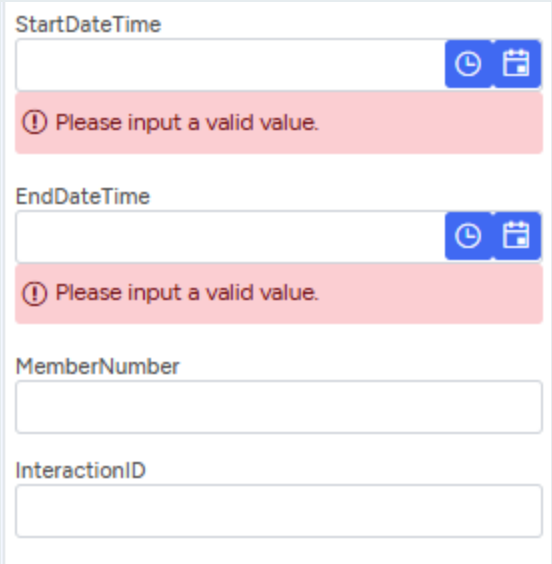
Tips for Users

- **Low offer rate** may indicate voice enrollment is disabled or underused.
- **High opt-out rate** suggests review of messaging or consent language.
- **High failure rate** may indicate poor audio, wrong member, or compromised account.
- Track trends before/ after script or policy changes.
- Pair with **Fraud Prevention – Activity by Source** to identify suspicious voice failures.
- Review monthly to ensure growth and stability of biometric adoption.

Report Options

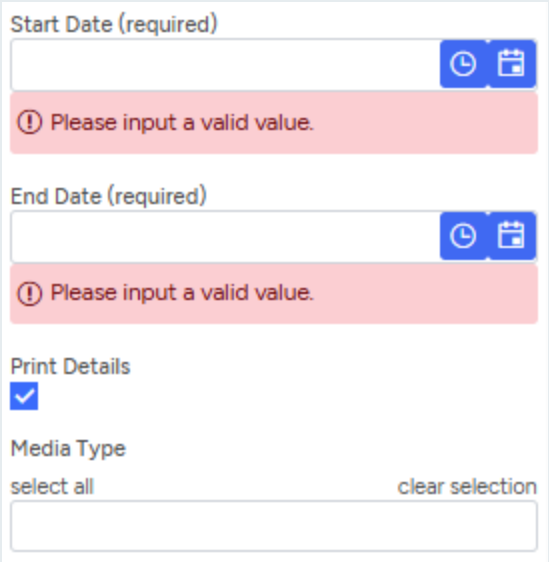
Filters

Apply filters to narrow down data, e.g., date range, member type, transaction type, interaction id etc.

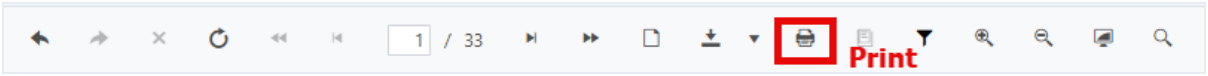


Sorting

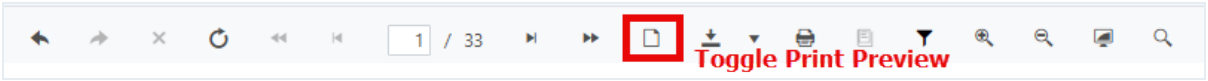
Sort data in different fields such as date, amount, member name.



Printing

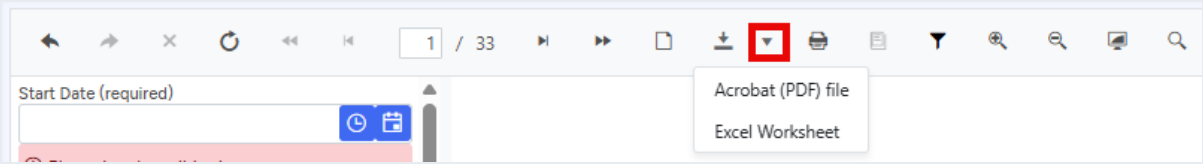
1. 

   Click on the **Print** button to print reports.

2. 

   Click on **Toggle Print Preview** to view the reports in Print style.

Exporting and Sharing Reports



1. **Export Formats** Reports can be exported in various formats such as **PDF** and **Excel** format.
2. **Sharing Options** Share reports via email or provide direct access through user permission.

Common Issues and Troubleshooting

Common Issues

- Report Generation Failure: Ensure all parameters are correctly set and that you have the necessary permissions.
- Data Discrepancies: Verify the data sources and refresh the data if needed.

Troubleshooting

- Check connectivity: Ensure a stable internet connection.
- Refresh the page and try again.
- Clear cache: Clear your browser cache if you encounter display issues.
- Contact support: Reach out to technical support for persistent issues.

Glossary

C

Consectetur

Definition for consectetur.

I

Ipsum

Definition for ipsum.

L

Lorem

Definition for lorem.

M

Maecenas

Definition for maecenas.

Maximus

Definition for maximus.