

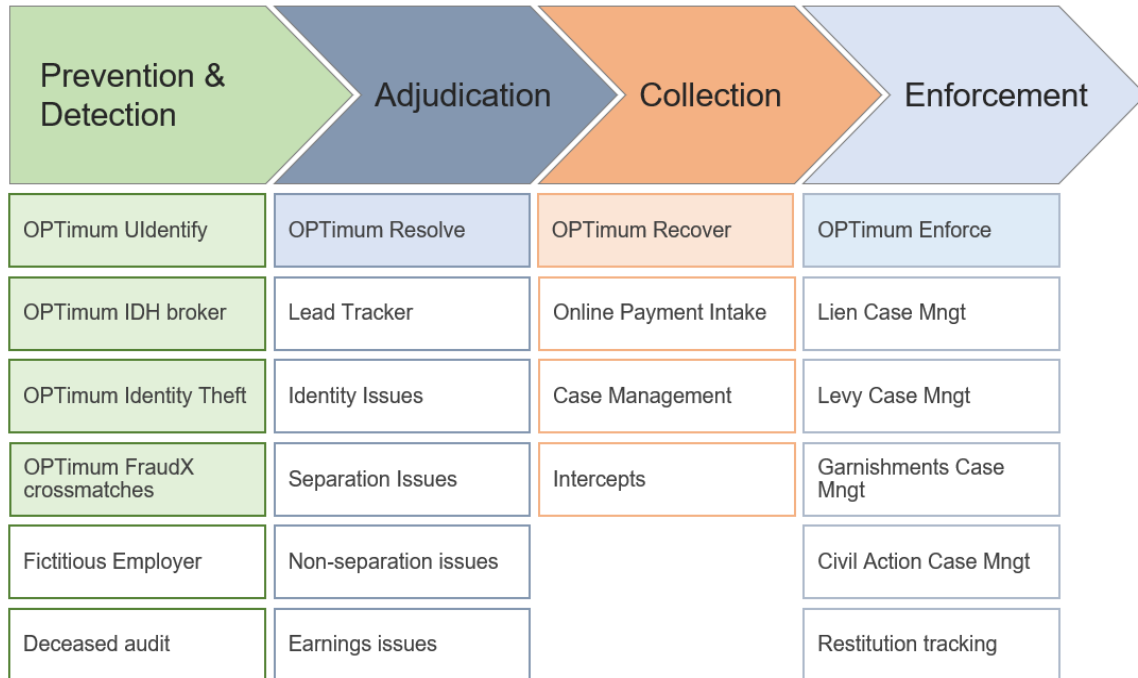
OPTimum Integrity Cloud



OPTimum Integrity Cloud (OIC)

- [What is the OPTimum Integrity Cloud?](#)
- How does it work?
 - [Backlog processing](#)
 - [Overpayment Workload Automation](#)
- Product details:
 - [UIdentify](#), [IDH Broker](#), [ID Theft](#), [Resolve](#), [Recover](#), [Enforce](#)
- What's the implementation strategy?
 - [Hosting, Security, and Technology stack](#)
 - Integration, rollouts and timelines
 - [Fraud Prevention](#)
 - [Workload automation](#)
 - [State resources needed](#)
- Who is On Point?
 - [Team On Point](#)
 - [Which states use On Point solutions](#)
- Insights
 - [Performance statistics](#)
 - [Demo recordings](#)
- [Frequently Asked Questions](#)

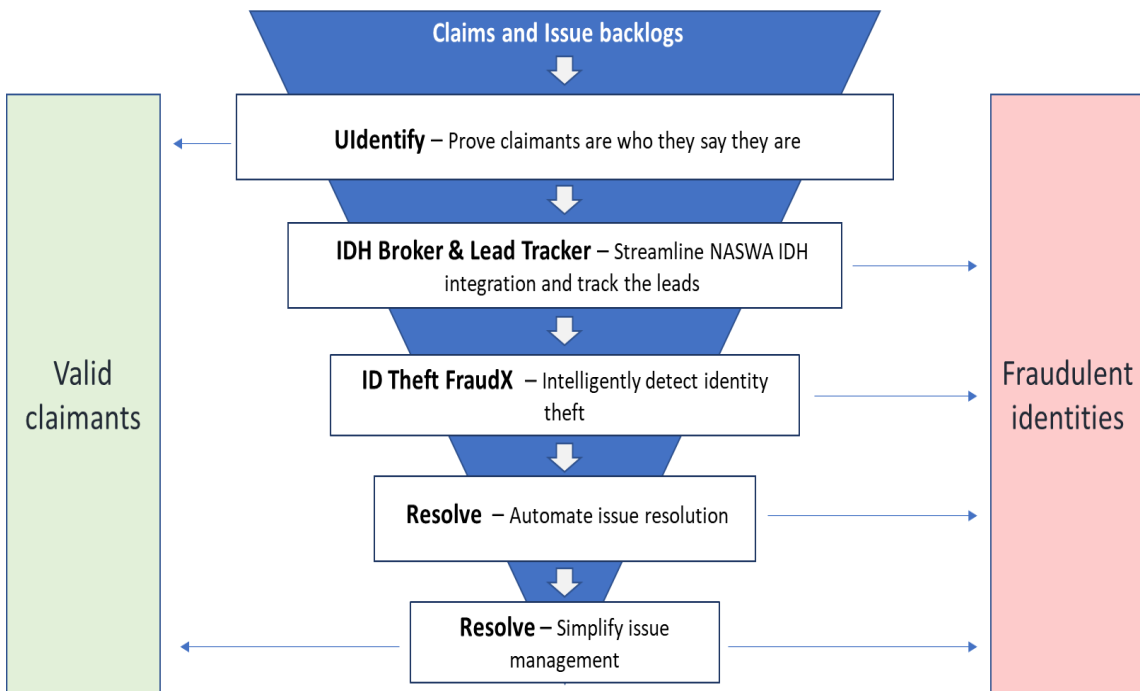
What is the OPTimum Integrity Cloud?



Shaded boxes depicts product, unshaded boxes depicts layers of functionality within a product

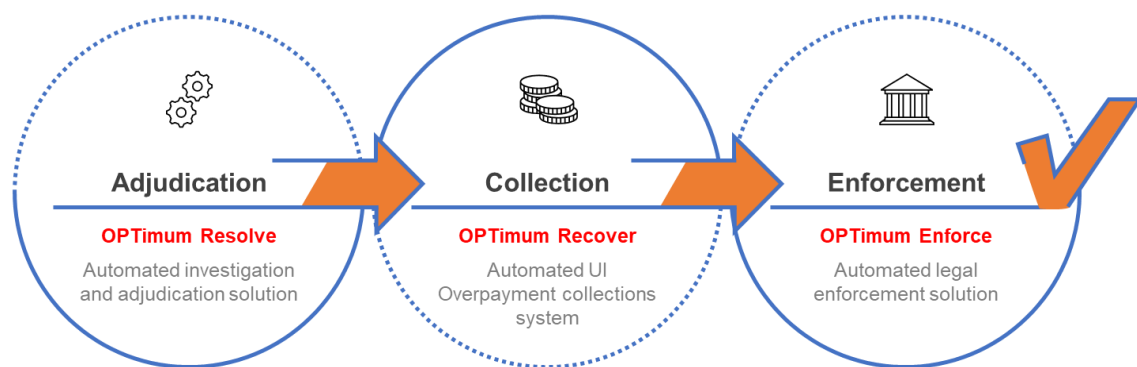
- The OIC is an enterprise solution that covers all UI integrity functions and objectives
- Built specifically for UI from day 1...none of this is ported of from another industry thus ensuring it really nails down the complexities of UI.
- Everything from prevention and detection to adjudication, collection, and legal enforcement.
- It's a holistic approach and solution but our layered strategy allows the state to pinpoint where to extend its current capabilities.
- Any of the individual solutions can be layered where needed allowing the state to continue using any systems and process that work well for you today.
- These solutions are helping states resolve massive backlogs, they're also being integrated as a part of claims processing.

A layered solution that Stops UI fraud



1. ID proofing solution enables the claimant to prove their identity.
 - **OPTimum UIdentify** matches a scanned ID against a national repository of DMV data to verify a claimant is who they claim to be. The only item a fraudster does not have is the physical ID.
 - States such as Arkansas make this a requirement of engaging with the state, thus avoiding expense adjudication processes.
 - Estimates show approx. 90% of working-class citizens possess a valid driver's license or state ID.
2. After filtering out validated claimants, interrogation of the remainder population occurs.
 - The **OPTimum IDH Broker** gives the agency access to NASWA's Integrity Data Hub. OIC streamlines integration with the IDH and provides lead tracking where investigators can manage hits. This is all live-in production within 2 weeks.
 - **OPTimum ID Theft** is a data analytics tool that leverages machine learning algorithms to detect identity theft patterns. Preconfigured with a proven model to identify fraud day 1 and it continues to grow in its capabilities as it detects fraud across the nation.
3. At this point in the flow, the state then has fraud scores associated with each of the claims. Based on state business rules, claims can be ranked by score and processed as follows:
 - **OPTimum Resolve** conducts automated claimant outreach through email, text message, or IVR integration. Then tracks responses and notifies states when it's clear to perform the non-responsive claimant procedures allowed by the state.
4. With validated claimants filtered, fraud deterred, and unresponsive claimants processed, left are the issues only adjudicators can solve.
 - **OPTimum Resolve** simplifies issue management guiding agency staff to achieve efficient, consistent, and accurate determinations.

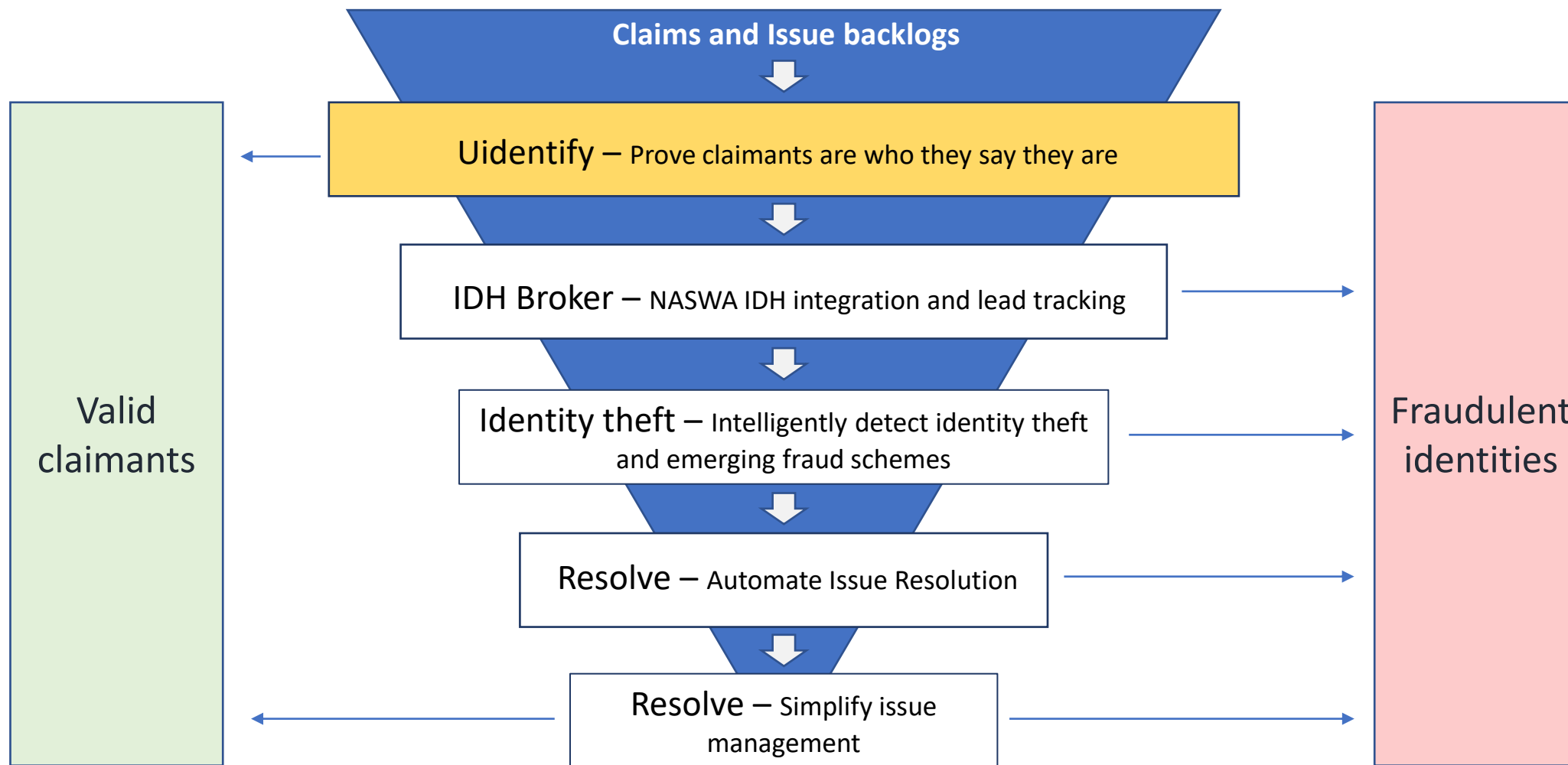
Overpayment workload automation



- Automate adjudication, collection, and enforcement processes.
- **OPTimum Resolve** automates fact finding, recommendations based on available evidence and establishes overpayments
 - The system generates tasks and sends out correspondence to the relevant parties and tracks the responses and determines next steps based on business rules. This trims the work associated with identity issues and allows agency staff to focus more of their time on more complicated issues.
- Collection of overpayments is automated by **OPTimum Recover**
 - The system determines whether a debt is collectible or not through a series of business rules then generates the appropriate collection notice and intercept activities.
- And lastly for Overpayments where collections activity are being ignored, automation of Legal remedies is performed by **OPTimum Enforce**.
 - The system identifies, creates, and manages legal actions based on business rules, configured to support Liens, Garnishments, Civil Actions, and Criminal Actions by breaking each legal action down into repeatable steps and proactively monitors each part such as document due dates, trial dates, and restitution details
- Stacking these solutions as such, creates workflows that squarely solve these major integrity goals
- OIC blocks fraud upfront, detects exceptions that slip through the cracks, and streamlines the integrity workload to keep the backlog low and the trust fund solvent.

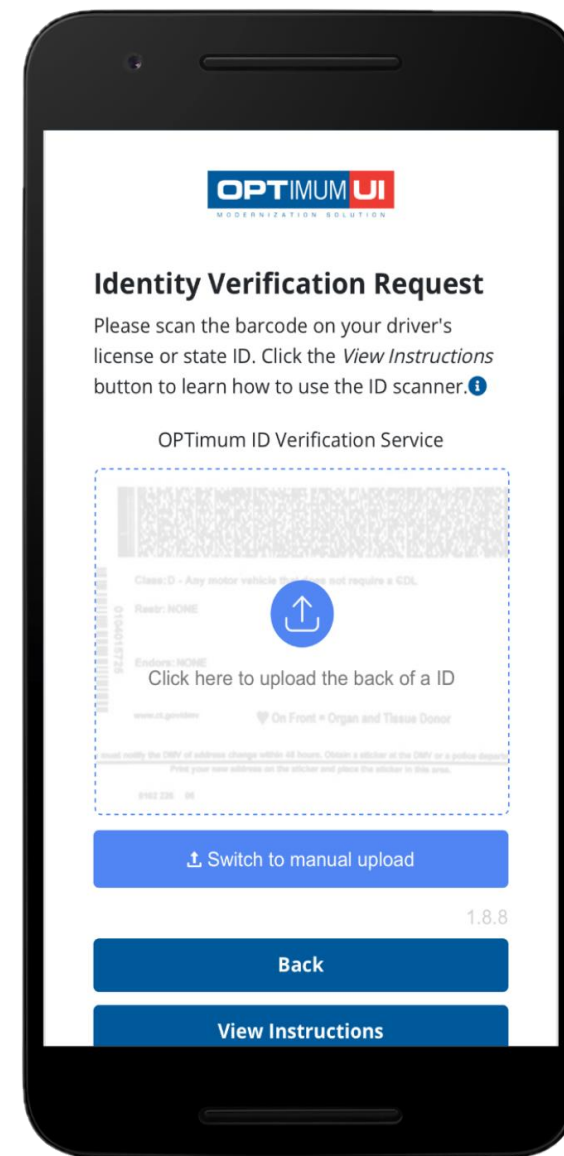
OPTimum Integrity Cloud

These solutions have been proven nationwide to prevent sophisticated fraud schemes and resolve claims and issue backlogs.



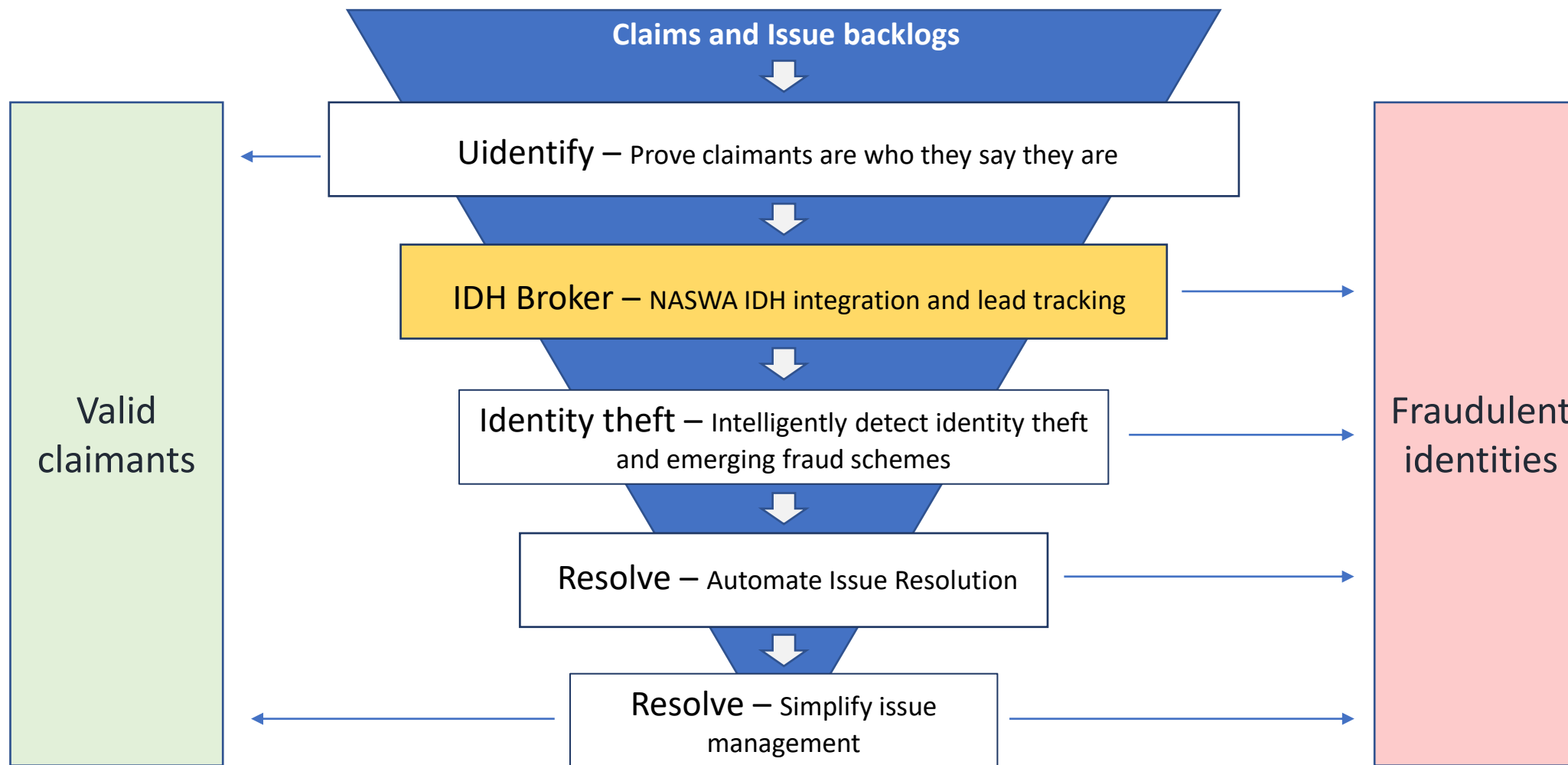
OPTimum UIdentify

- Identity proofing solution that utilizes AAMVA Driver's License Data Verification, document format validation, and third party verification sources
- Browser-based live ID barcode scan that is quick and easy
- Agency portal to manage all UIdentify requests
- Lowest price in the industry for live scan identity proofing



OPTimum Integrity Cloud

These solutions have been proven nationwide to prevent sophisticated fraud schemes and resolve claims and issue backlogs.



OPTimum IDH Broker

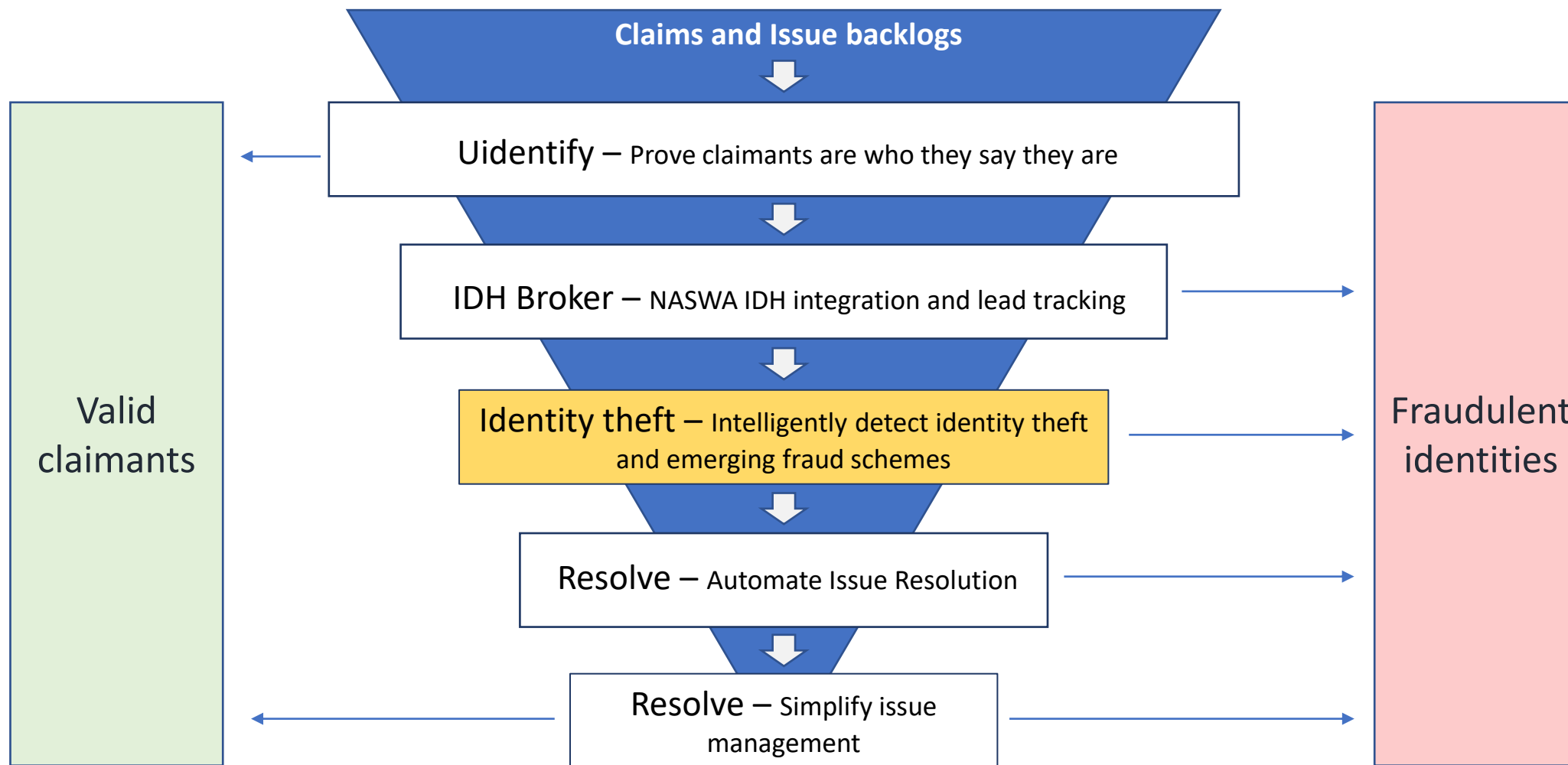
The screenshot shows the OPTimum UI interface. On the left is a blue sidebar with navigation options: LEADS, Home, Integrity Data Hub, IDH Home, Report to IDH, Submitted Reports, Pending Reports, IDH Lookup, IDH Crossmatch, IDH Crossmatch Summary, Sent Record Details (selected), Real time Lookup History, Identity Theft, and Healthcare Employer Fraud. The main content area shows the 'Sent Record Details' page for a user named NORM HARELIK. The page title is 'Home / Integrity Data Hub (IDH) Crossmatch / IDH Crossmatch Summary / Sent Record Details'. Below the title is a description: 'Displays a list of crossmatch actors sent to IDH database for crossmatching.' There is a 'Search and Sort' button and a 'Number of Rows Per Page' dropdown set to 10. The main table has the following data:

Claim ID / Unique ID	Claimant Name	IDV Score	IDV Synthetic Indicator	Date of Birth	Claim Type	Actions
CLAIM_9312578	JOHN DOE	150	Yes	07/03/1985	Initial	View IDH Response
IDV Review Indicator		Yes				
Program Type		Regular Unemployment Insurance				
Occurrence Date		03/07/2020				
Effective Date		04/07/2020				
SSN		XXX XX 2752				
Email		john.doe@idhba.com				
IP Address		71.12.124.114				
Address 1		100 Millard Avenue Keene, MA 03490				
Address 2		124 Highland Place Keene, MA 03417				
Phone 1		(813) 541-146				
Phone 2		963-759-979				
Phone 3		281-967-028				
Direct Deposit Routing Number						
Direct Deposit Account Number						
> CLAIM_9316886	WHEBE HILLAND	150	Yes	08/18/1973	Initial	View IDH Response
> CLAIM_9657180	DARRELL R. FORTIN	150	Yes	10/08/1969	Initial	View IDH Response
> CLAIM_9348577	CLAYTON BASS	170	Yes	04/24/1977	Initial	View IDH Response

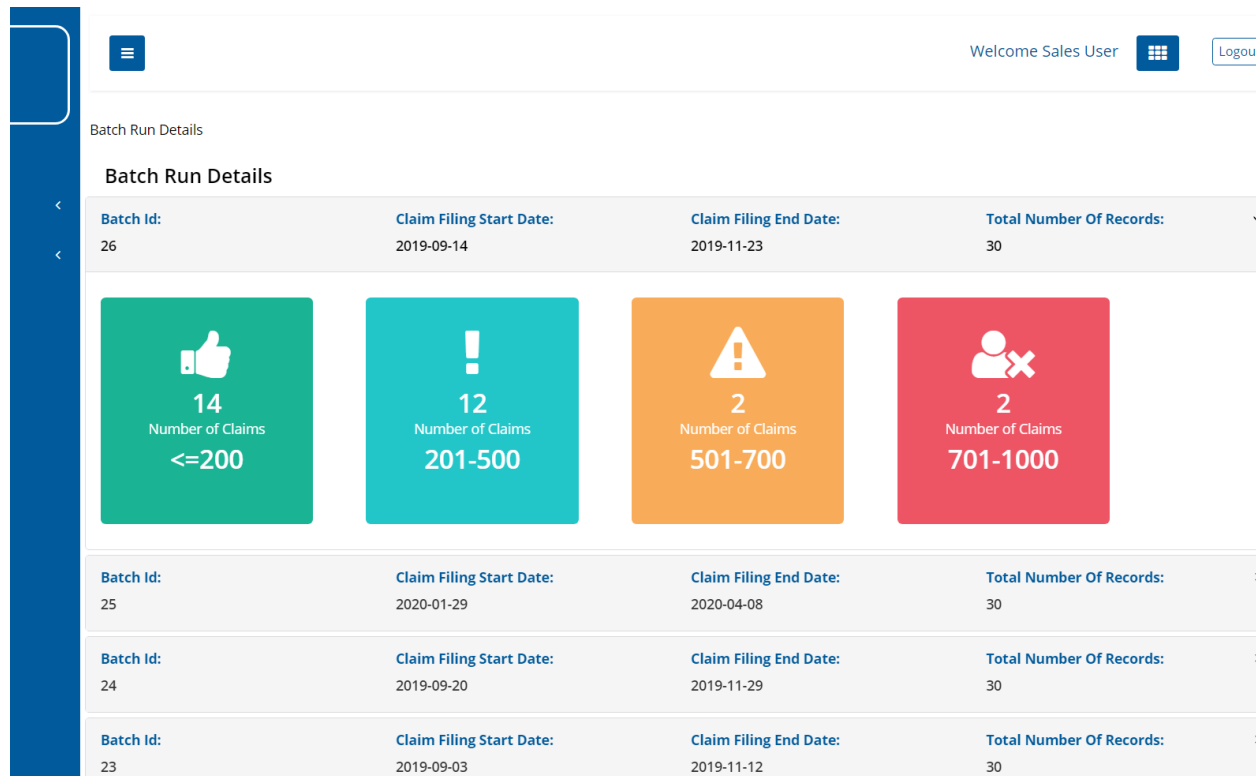
- Streamline entire integration between SWA and NASWA IDH
- Implementation of initial rollout is live within 2 weeks
- Intuitive UX that consolidates all requests and responses
- Easily prioritize leads and expediate investigations
- Aligned with NASWAs IDH Roadmap

OPTimum Integrity Cloud

These solutions have been proven nationwide to prevent sophisticated fraud schemes and resolve claims and issue backlogs.

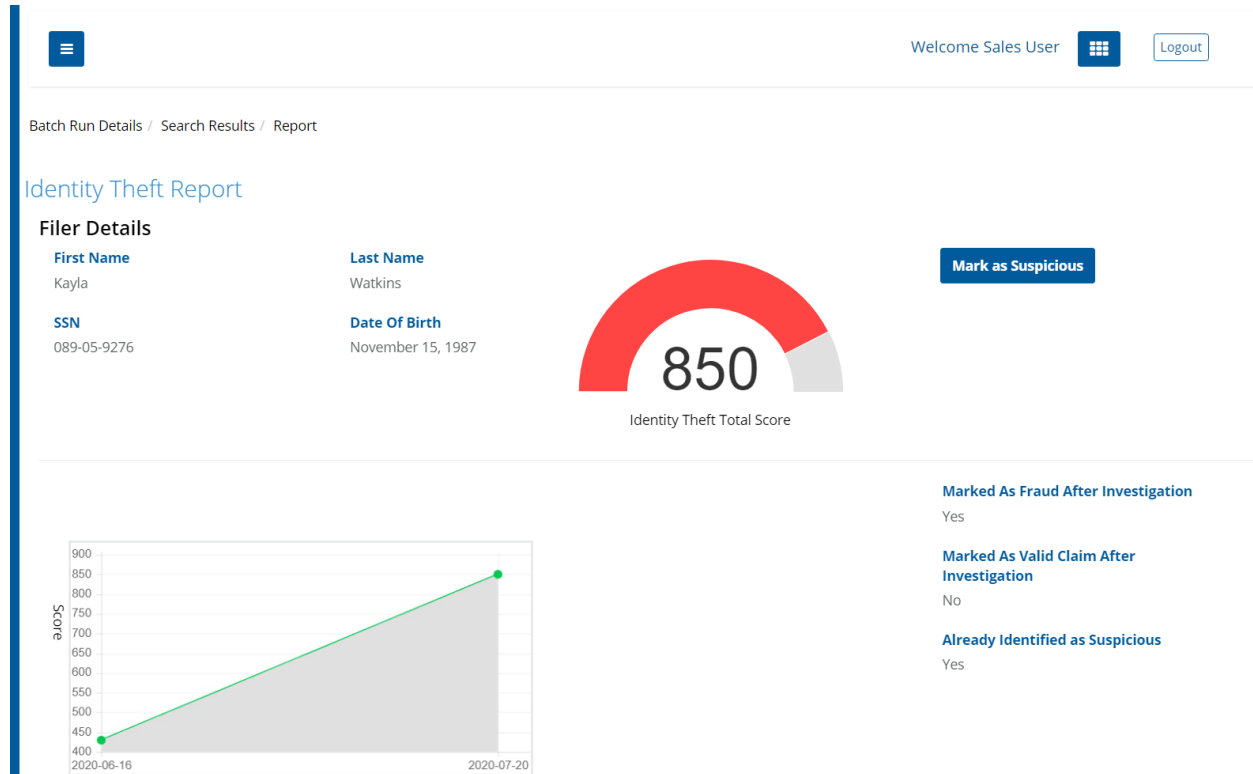


OPTimum Identity Theft



- Creates and refines a database of known bad actors
- Leverages decades of UI fraud investigative knowledge combined with data science
- Batch results are scored and grouped
- Proven product with over \$184MM saved

Scoring



- Scoring attributes consist of 11 categories of data
- Investigators can flag accounts for investigation and boost the scoring algorithm by providing investigation results
- Scoring trends tracked over batch run cycles to quickly see pattern shifts

Staying one step ahead

The screenshot displays the 'AGENCY PORTAL' interface for 'OPTIMUM UI'. The left sidebar contains navigation options: Home, Identity Theft, Identity Theft Settings (selected), Suspicious Email Domains, Suspicious ISPs, Known IP Address, Scoring Adjustment, Admin, and IDV Request. The main content area is titled 'Suspicious Email Domains' and includes a sub-section 'Add New Suspicious Email Domains' with an input field and an '+ Add' button. Below this is the 'Show Suspicious Email Domains' section, which has 'Show Active' and 'Show History' buttons. A table displays the active domains:

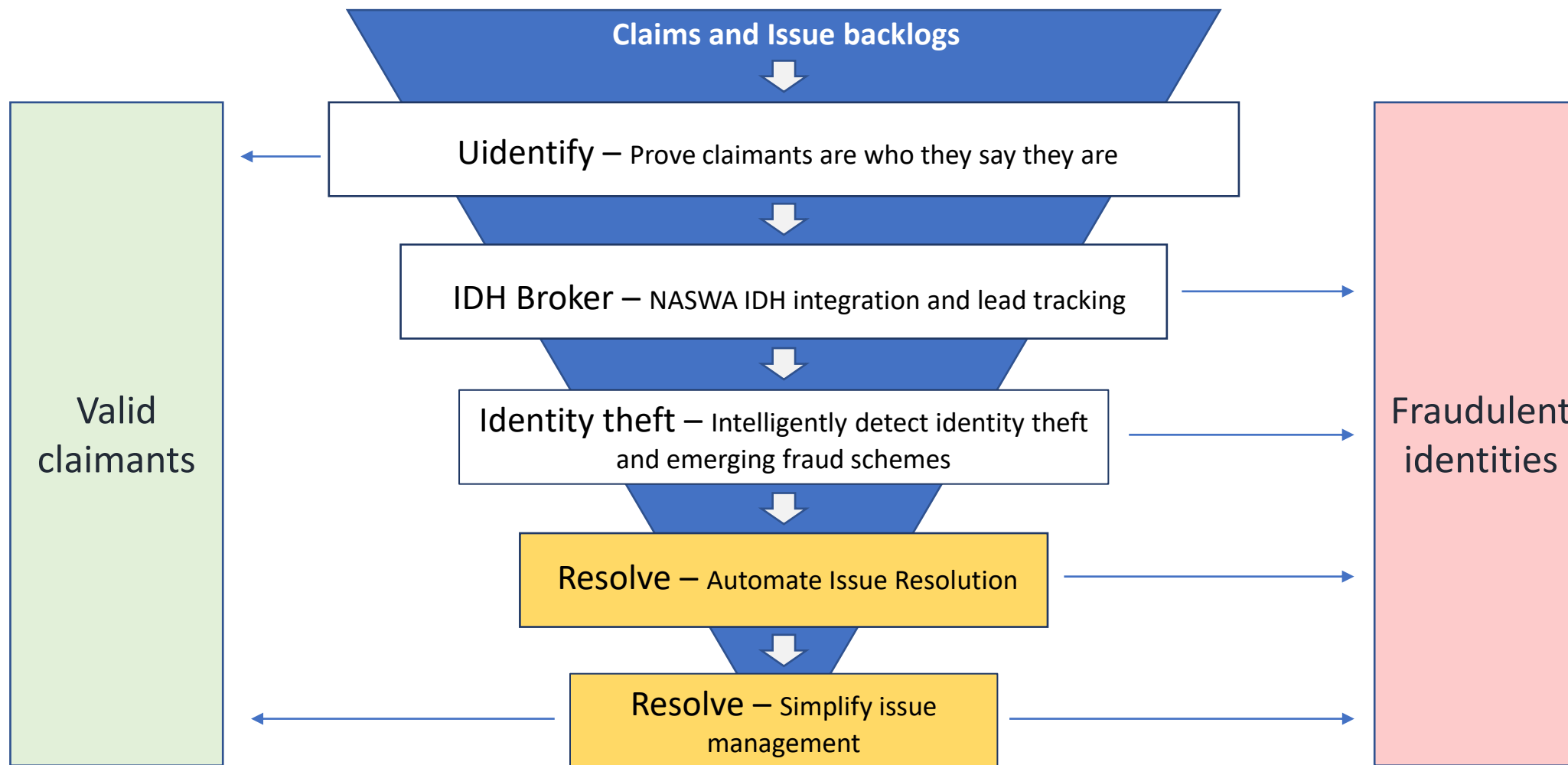
Id	Grey Email Domain	Record Added By	Record Added Time
1	getnada.com	rajeev1	2020-06-18 03:46:18
3	mailinator.com	rajeev	2020-06-22 10:55:38

At the bottom of the table, it indicates 'Total Items: 2'.

- Intelligence and feedback loop built-in to refine existing model and detect emerging fraud patterns
- Empower investigators and enrich the dataset
- Add suspicious email domains and ISPs
- Ignore IP Addresses to prevent false positives
- Make scoring adjustments as needed

OPTimum Integrity Cloud

These solutions have been proven nationwide to prevent sophisticated fraud schemes and resolve claims and issue backlogs.



OPTimum Resolve - FastPath

Resolve

Resolve

Claimant Overview

Benefit Year History

Issue List

Task List

Assigned Tasks

Search

NORM HARELIK Logout

Welcome to the Resolve application!

The OPTimum Resolve application is a case management system designed to provide your state workforce agency with the tools necessary to efficiently manage benefit claim issues and improve the integrity of the unemployment insurance program. This application allows you to create and track the progress of the non monetary issues and it determines an intelligent workflow for appropriate users to efficiently conduct fact finding and collect data to process an issue resolution in a timely manner.

Resolve Overview

Assigned Tasks

Displays all tasks assigned to you. Click the 'View' action button to view details of the task.

Number of Rows Per Page: 5

Task Name	Date Created	Date Assigned	Assigned To	Status	Due Date	Action
Review Issue Resolution	08/14/2020	08/14/2020	NORM HARELIK	Pending	08/24/2020	View
Task Description	Review required on determination based on available evidence for an issue on "Rapid Review".					
Task Type	Review Issue Resolution					
Created By	SYSTEM					
Last Updated On	08/14/2020					
Last Updated By	08/14/2020					
Issue Not Assigned Task	08/13/2020	08/13/2020	SYSTEM	Pending	08/24/2020	View
Task Sample 3	08/11/2020	08/11/2020	SYSTEM	Pending	08/21/2020	View
Task Sample 2	08/11/2020	08/11/2020	SYSTEM	Pending	08/21/2020	View
Task Sample 1	08/11/2020	08/11/2020	SYSTEM	Pending	08/21/2020	View

- Full case management for identity issues
- Intelligent issue assignment
- FastPath processing

Intelligent Fact-Finding

OPTIMUM UI

Resolve

Resolve

Claimant Overview

Issue Details

Record Fact Finding

Issue Narrative

Issue Activity

Benefit Year History

Issue List

Task List

Assigned Tasks

Home / James Smith / Issue Details / Record Fact Finding

Record Fact Finding

Issue Information

Issue ID	105	Assigned To	Norm Harelík
Issue Type	Identity Issue	Timeliness Due Date	08/21/2020
Established Date	08/11/2020	Detection Date	08/11/2020
Issue Effective Date	08/09/2020		
Source	ID Theft Crossmatch	Program	REG - UI

Fact Finding Information

Please provide the details of the fact finding.

Created On 08/12/2020 **Created By** Norm Harelík

***Description**

This is sample facts of the case.

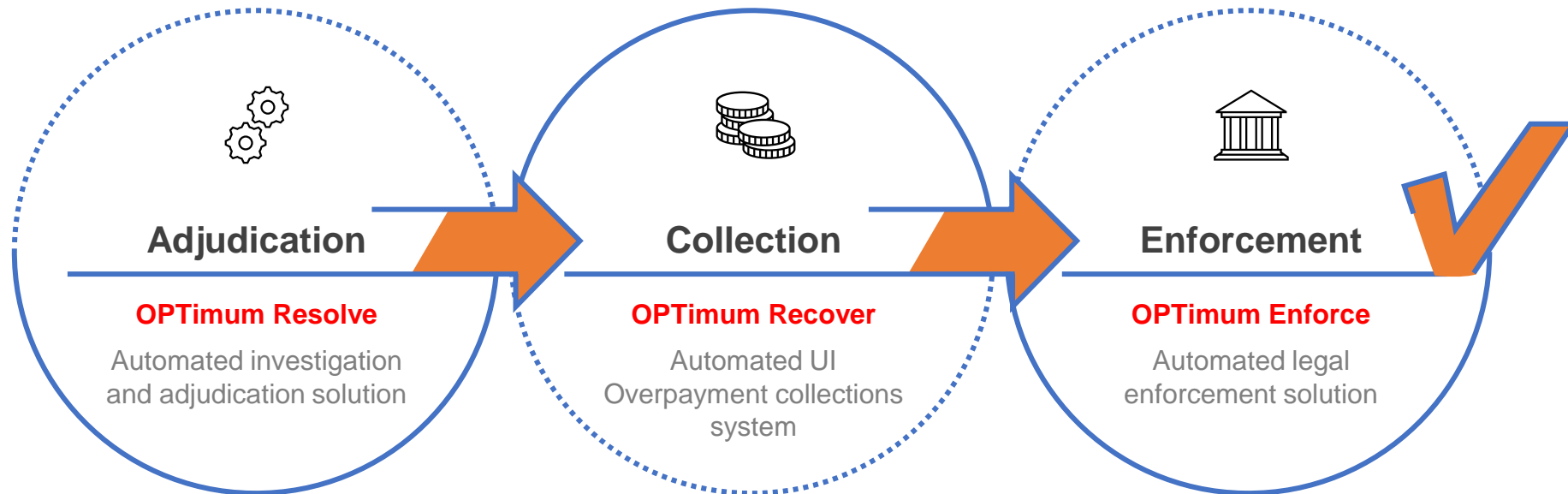
- Streamlined fact-finding
- Evidence upload supported
- Direct access to issue artifacts

Simple and Comprehensive

The screenshot displays the 'OPTIMUM UI' interface. On the left is a blue sidebar with a 'Resolve' button and a menu containing: Resolve, Claimant Overview, Issue Details (selected), Issue Narrative, Issue Activity, Benefit Year History, Issue List, Task List, and Assigned Tasks. The main content area features a breadcrumb trail 'Home / James Smith / Issue Details' and a progress bar with six stages: Detected (checked), Rapid Review (checked), Fact Finding (checked), Resolution (active), Determination, and Completed. Below the progress bar are sections for 'Issue Details', 'Issue Information' (a table with fields like Issue ID, Issue Type, Established Date, Issue Effective Date, Source, Assigned To, Timeliness Due Date, Detection Date, and Program), 'Identity Verification Requests' (with a filter dropdown set to 'Requested' and a message 'No identity verification requests to display'), and 'Issue Documents'.

Issue Information			
Issue ID	105	Assigned To	Norm Harelik
Issue Type	Identity Issue	Timeliness Due Date	08/21/2020
Established Date	08/11/2020	Detection Date	08/11/2020
Issue Effective Date	08/09/2020		
Source	ID Theft Crossmatch	Program	REG - UI

- Business process engine guides staff through issue resolution
- Consistent and reliable determinations
- Comprehensive issue details in one place



OPTimum Recover

OPTIMUM UI

Recover

Home

Recover Home

Account Management

Search

NORM HARELIK Logout

Welcome to the Recover application!

The OPTimum Recover application is a case management system designed to provide your state workforce agency with the tools necessary to maximize overpayment recoveries, protect the Unemployment Insurance (UI) trust fund, and improve the integrity of the UI program. This application allows you to capture, track, and manage the recovery of UI benefits through an intelligent and cost effective billing cycle.

Recover Overview

Assigned Tasks

Displays all active tasks assigned to you. Click the 'View' action button to view details of the task.

Task Name	Date Created	Date Assigned	Assigned To	Status	Due Date	Action
▼ New Hire Crossmatch Hit	05/25/2020	05/25/2020	NORM HARELIK	Open	06/24/2020	View
Task Description	New Hire xmatch results: Obtained address from New Hire Crossmatch: 23 CHARLES STREET WALKER HELENA, GA, 35080. Claimant New Hire date was found to be 05/01/2020. This is additional text for testing the ...					Show More
Task Type	New Hire Crossmatch Hit					
Created By	SYSTEM					
Last Updated On	05/25/2020					
Last Updated By	05/25/2020					
Misdemeanor - 6 months	05/25/2020	05/25/2020	NORM HARELIK	Open	06/24/2020	View
▶ Felony - 6 Months	05/26/2020	05/26/2020	NORM HARELIK	Open	06/25/2020	View
▶ Felony - 12 Months	05/27/2020	05/27/2020	NORM HARELIK	Open	06/26/2020	View
▶ Balance Exceeds Threshold	05/27/2020	05/27/2020	NORM HARELIK	Open	06/26/2020	View

- Software to automate and manage overpayment collections
- Generate collections related notices and documents
- Complete account inquiry capabilities
- Monitor address changes and NDNH/SDNH hits
- Optional Claimant Payment Portal

FastPath

Account Information

Close Date	Not Available	Original Overpayment Amount	\$2,600.00
Last Refresh Date	06/22/2020	Total Collectible Amount	\$2,600.00
Assigned User	NORM HARELIK	Collectible Principal Balance	\$2,250.00
Path	Auto-Recovery	Collectible Penalty Balance	\$195.00
Minimum Payment Override End Date	Not Available	Collectible Interest Balance	\$0.00
Last Wage Quarter	Not Available	Collectible Fees Balance	\$55.00
Total Last Quarter Wage	Not Available	Total Collectible Balance	\$2,500.00
		Minimum Payment Due	\$2,500.00

Overpayment Information

Displays the claimant's overpayment balance.

- Auto-Recovery

- Account fully automated
- Generation of all collection notices
- Intelligent assignment of tasks

- Directed-Recovery

- Account assigned based on business rules
- Returned to Auto-Recovery when business rules are met

Claimant Overpayment Payment Portal

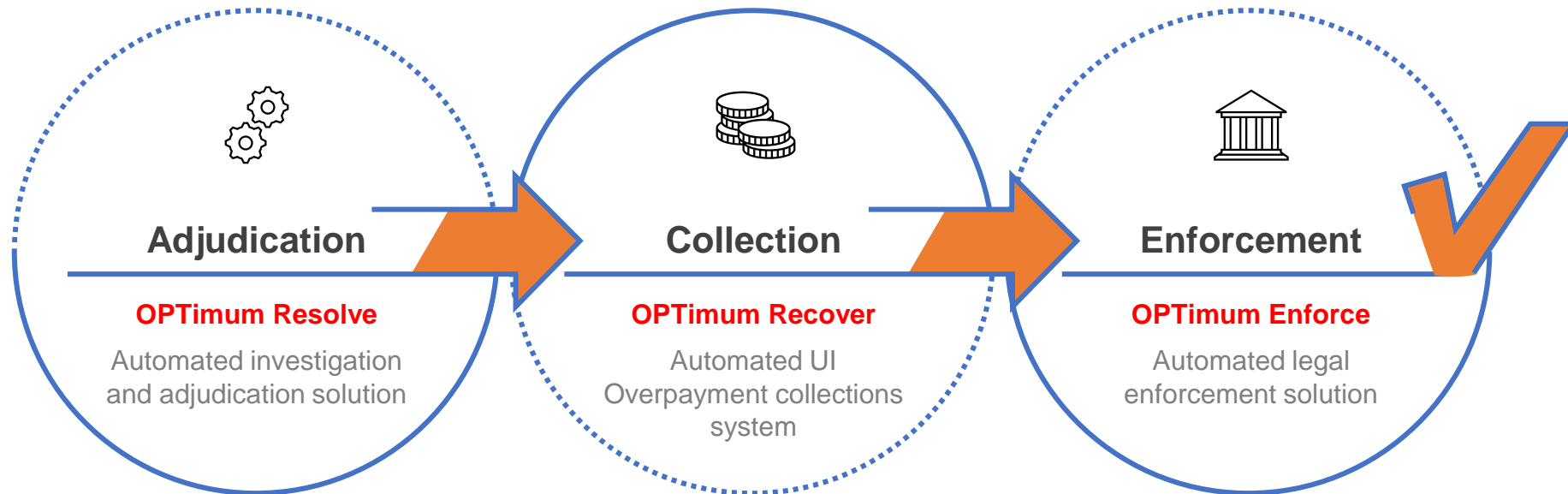
The screenshot shows the 'CLAIMANT PORTAL' interface. On the left is a blue sidebar with the 'OPTIMUM UI' logo and navigation links: Home, My Profile, My Documents, Billing History, Overpayment Information, Repayment Information, and Contact Agency. The main content area has a header with a hamburger menu, 'Welcome JAMES', and a 'Logout' button. Below the header is a 'Required Actions' section with a 'Task Name' box containing a message about an outstanding benefit overpayment balance due by 06/23/2020, with a 'Make Repayment' button. This is followed by an 'Account Balance' section with a summary table and a 'Make Repayment' button. The 'Overpayment Information' section contains a table with columns for Established Date, Program, Fraud Indicator, Original Total Principal Amount, Original Total Penalty Amount, Original Total Fees Amount, Original Total Amount, Status, and Action.

Minimum Amount Due	Repayment Due Date	Total Amount Due	Action
\$2,500.00	06/23/2020	\$2,500.00	Make Repayment

Total Principal Balance	Total Interest Balance	Total Penalty Balance	Total Fees Balance
\$2,250.00	\$195.00	\$55.00	\$0.00

Established Date	Program	Fraud Indicator	Original Total Principal Amount	Original Total Penalty Amount	Original Total Fees Amount	Original Total Amount	Status	Action
12/12/2019	UI	Fraud	\$1,600.00	\$50.00	\$0.00	\$1,800.00	Collectible	View Repayments
Current Total Principal Balance			\$1,600.00					
Current Total Interest Balance			\$150.00					

- Stand-alone or integrated within the state's current claimant interfaces.
- Instant access to up-to-date overpayment balance information and repayment history
- View and download all collections correspondence
- Email/SMS alerts
- Make one-time online payments
- Manage profile and contact information



OPTimum Enforce

The screenshot displays the ENFORCE software interface. At the top, there is a navigation bar with the ENFORCE logo and the tagline 'AN ON POINT TECHNOLOGY SOLUTION'. Below this, there are tabs for 'Case Management', 'System Administration', 'Reports', and 'Manage Reference Data'. The main content area is titled 'My Cases' and features a 'Filter Cases' section with dropdown menus for 'Workunit' and 'User', and a checkbox for 'Include Closed Cases?'. Below the filter section is a table of 'Open Cases' with the following data:

Case ID	SSN	Claimant Name	Case Type	Case Status	Principal Balance	Court Name	Assigned User
5	059606356	DARIUS A BROWN	Civil Action	Open	50.00	Magistrate Court of Houston County	Suzanne DelaCruz
2	054687030	LINDA K BRANCH	Civil Action	Open	0.00	Magistrate Court of Cobb County	Suzanne DelaCruz
2	061625425	ONIKA K TRICE	Civil Action	Open	0.00	Magistrate Court of Douglas County	Suzanne DelaCruz
3	036424226	JOANN HEATH	Civil Action	Open	1799.00	Magistrate Court of Lowndes County	Suzanne DelaCruz
3	054687030	LINDA K BRANCH	Criminal Action	Open	0.00	State Court of Cobb County	Suzanne DelaCruz

At the bottom of the table, there are search filters for Case IDs, SSNs, Names, Case Types, Case Statuses, Balances, Court Names, and Users. A 'Reassign Cases' button is located at the bottom right of the table area.

- Identifies, creates and manages cases based on established business rules
 - Liens
 - Garnishments
 - Civil Actions
 - Criminal Actions
- Proactively monitors legal action workflow steps
- Automatically creates customized documents and notices to court officials, claimants, and employers

FastPath

The screenshot displays the ENFORCE Case Management interface. At the top, there is a navigation bar with the ENFORCE logo and the tagline "AN ON POINT TECHNOLOGY SOLUTION". The main navigation menu includes "Case Management", "System Administration", "Reports", and "Manage Reference Data". The current page is titled "Case Details" and shows information for Case ID 5. The case is a Civil Action, currently Open, created on 01/02/2020, and assigned to Suzanne Delacruz. The claimant is DARIUS A BROWN, residing at 111 BRANDYWINE, WARNERROBINS, AL 31088. The original case balance is \$55.00. The workflow history shows a step "File Default Judgment" completed on 07/16/2020. The open tasks table lists "File Default Judgment" with a due date of 07/21/2020 and "Case Setup" with a due date of 01/15/2020.

Case Summary			
Case ID:	5	Case Type:	Civil Action
SSN:	059606356	Case Status:	Open
Claimant Name:	DARIUS A BROWN	Case Creation Date:	01/02/2020
Claimant Address:	111 BRANDYWINE, WARNERROBINS, AL 31088	Assigned User:	Suzanne Delacruz
Original Case Balance:	\$55.00		

Open Tasks			
Task Subject	Assigned Date	Due Date	
File Default Judgment	07/16/2020	07/21/2020	
Case Setup	01/10/2020	01/15/2020	

- Creates cases without staff intervention
- Assigns cases to the appropriate court
- Alerts staff of missed due dates and deadlines as well as other failed responses
- Takes actions based on overpayment balances and repayments
- Automatically closes cases and releases liens, garnishments or other court orders

Hosting & Subscription model

Subscription

- Worry Free administration
- Continuous Monitoring
- Product Road Map based upgrades
 - Annual dot releases and hot fixes
 - Annual major release
- State based security guidelines
- Proactive customer service
- Monitored Service Level Agreements

Hosting/Security

- Hosting is FedRAMP moderate and can be hosted within AWS GovCloud
- Hardware/environment agnostic design through Docker Containers
- Can be installed
 - on-premise
 - AWS Cloud, Google Cloud, Azure Cloud
 - or any compliant & FedRAMP certified IaaS cloud vendor

Single Tenant SaaS Model

- Software instance is not shared.
- Dedicated environment per client.
- Limited client customizations
- Improved Security
 - Customer's data is completely isolated from others
 - Isolated Virtual Private Cloud (VPC)
- Reliable Operations
- Flexibility in migration

Integration and rollout strategy

Prevention / Detection

The implementation roadmap gives states access to powerful tools quickly and the grows the level of integration as the state's priorities require.

- Products get deployed early in the project, usually within 2-3 weeks of project launch.
- Early roll-outs require little-to-no integration. States users gain access to much needed defenses instantly.
- Subsequent roll outs progress into uploading/FTP of batch files extracted from the state's systems.
- Automated data transfers and automation of actions between systems are jointly developed by state IT/On Point concurrent to prior roll outs and deployed according to priority of the state.

Levels of Integration	OPTimum UIdentify	OPTimum IDH SAR Broker	OPTimum ID Theft
Base Implementation	3 weeks (from start of scheduled layer)	2 weeks (from start of scheduled layer))	2 weeks (from start of scheduled layer)
State instance live in Prod			
Manual entry of input data			
Access results though GUI and Reports			
Batch Processing	1 week (after base implementation)	2 weeks (after base implementation)	3 weeks (after base implementation)
Extract of data loaded for processing			
Access results though GUI and Reports			
Automated data transfers	3 weeks (after batch implementation)	3 weeks (after batch implementation)	3 weeks (after batch implementation)
Data transfers from state systems automated			
Results published to state systems automated			

Integration and rollout strategy

Workload Automation

The implementation roadmap gives states access to powerful tools quickly and the grows the level of integration as the state’s priorities require.

- Process automation requires stronger outlines of current process flows and alignment
- Base system implementation becomes available to state early in the project
- Subsequent roll outs allows for data integration and alignment
- Automated data transfers and automation of actions between systems are jointly developed by state IT/On Point concurrent to prior roll outs and deployed according to priority of the state.

Case Automation / Integration	OPTimum Resolve	OPTimum Recover	OPTimum Enforce
Base Implementation / OIC tools availability	3 weeks (from start of scheduled layer)	6 weeks (from start of scheduled layer)	3 months (from start of scheduled layer)
State instance live in Prod			
Initial issue type process automation			
Access results though GUI and Reports			
Batch Processing / Data alignment / Process Automation	2 weeks (after base implementation)	4 weeks (after base implementation)	1 Month (after base implementation)
Issue automation process implementation			
Access results though GUI and Reports			
Automated data transfers	6 weeks (after batch implementation)	2 weeks (after batch implementation)	2 weeks (after batch implementation)
Data transfers from state systems automated			
Results published to state systems automated			

State IT/SME team capacity needed

The rollout plan allows the state to deploy the fraud protection most urgent while managing team member availability.

Each horizontal integration below assumes the vertical product is being deployed independently, there's efficiencies when rolling out multiple products

**rough order of magnitude estimates can increase or decrease based on state data accessibility/complexity*

Levels of Integration	OPTimum UIdentify	OPTimum IDH SAR Broker	OPTimum ID Theft	OPTimum Resolve	OPTimum Recover	OPTimum Enforce
Base Implementation	IT – 32 hours SME – 64 hours	IT – 32 hours SME – 40 hours	IT – 48 hours SME – 64 hours	IT – 40 hours SME – 80 hours	IT – 40 hours SME – 80 hours	IT – 80 hours SME – 120 hours
State instance live in Prod						
Manual entry of input data						
Access results though GUI and Reports						
Batch Processing	IT – 16 hours SME – 16 hours (in addition to base implementation)	IT – 16 hours SME – 16 hours (in addition to base implementation)	IT – 24 hours SME – 8 hours (in addition to base implementation)	IT – 24 hours SME – 8 hours (in addition to base implementation)	IT – 40 hours SME – 80 hours (in addition to base implementation)	IT – 64 hours SME – 80 hours (in addition to base implementation)
Extract of data loaded for processing						
Access results though GUI and Reports						
Full Integration	IT – 40 hours SME – 40 hours (in addition to batch implementation)	IT – 24 hours SME – 32 hours (in addition to batch implementation)	IT – 16 hours SME – 24 hours (in addition to batch implementation)	IT – 80 hours SME – 80 hours (in addition to batch implementation)	IT – 80 hours SME – 80 hours (in addition to batch implementation)	IT – 80 hours SME – 80 hours (in addition to batch implementation)
Data transfers from state systems automated						
Results published to state systems automated						

Team On Point

Over the past 30 years On Point has been developing and managing integrity solutions for SWAs

Team members that span the nation totally centuries of UI experience.

We get UI, since our inception it's 100% of our business.

Sample of our UI Expertise

- Chief of Investigations (Washington ST) - [Kathy Moore](#)
- Manager of Benefit Systems (Illinois) - [Norm Harelik](#)
- UI Director (Virginia) - [Becky Sperlazza](#)
- Director of Tax Operations (Massachusetts) - [Joe Pacheco](#)
- Assistant UI Commissioner (New Jersey) - [Bob Yokavonus](#)
- CIO (New Jersey and NASWA) - [Joe Vitale](#)
- IT Solutions Provider (New Jersey and NASWA) - [Tom Kusnirik](#)
- Deputy Administrator, USDOL (Washington ST and Maryland) - [Dale Ziegler](#)

Current installations

	Cloud solutions					On-premise solutions								
	Uidentify	ID Theft	Resolve	IDH Broker	FraudX Audit	BARTS	BARTS DB	IRME	AWARE	RECOVER	ENFORCE	NORM (CORE)	OPTIMUM XMATCH	Workforce Reporter
Alaska						X	X		X					
Arizona		X		X	X	X	X	X						
Arkansas	X		X	X		X	X	X		X	X	X		
DC						X				X				
Georgia						X	X		X	X	X			
Illinois						X								
Kentucky						X	X	X		X				
Louisiana									X					X
Massachusetts				X					X					
Nevada														X
New Jersey						X		X						
South Carolina													X	
Puerto Rico						X				X				
Texas									X					

Performance statistics

State A was buried with a sizable backlog of claims they suspect was largely fraud.

- After filtering through UIdentify over 10% of the claims were discovered to be valid claimants. Those claims were quickly cleared and deserving claimants began receiving benefits.
- The solution will block the fraud they already suspected in that pool and any claims that result in an issue will be efficiently processed by Resolve.
- Trends are showing approximately 48,000 claims will go through the Resolve automated non-responsive claimant path, with an MPU of 40 minutes State A stands to save over 39,000 hours of work.

State B began to encounter that 70% of their initial claims over a period of a few weeks were hitting fraud score thresholds.

- Both the IDH broker and audits available within our ID Theft product are detecting the fraud claims and enabling the claims to be blocked.

State C using an audit available in our ID Theft solution discovered a pattern of debit cards, bank type, and address gave indication of fraud

- The ID Theft audit over a 2 month timeframe detected fraud and enabled the state to stop paying \$22,049,595 in weekly claims. This would have resulted in over \$1.1B in fraud if the claims were allowed to exhaust their benefits.

Demo recordings / Customer testimony

OPTimum customer testimonial

- MA Integrity Director Brian O'Connell provides testimonial during OIC webinar

[Click here for recorded testimonial \(4:20 min\)](#)

OPTimum IDH broker

- Demo of SAR integration, IDV release not available at time of this recording

[Click here for recorded demo of IDH broker \(13:12 min\)](#)

OPTimum Resolve

- Demo of adjudication automation solution

[Click here for recorded demo of OPTimum Resolve \(4:51 min\)](#)

OPTimum Identity theft

- Demo of batch mngt, fraud report, and score tuning

[Click here for recorded demo of ID Theft \(15:52 min\)](#)

OPTimum UIdentify

- Demo of solution integrated to allow on demand id proofing by a state user.

[Click here for recorded demo of UIdentify on-demand \(2:07 min\)](#)

OPTimum UIdentify

- Demo of solution integrated within claims intake

[Click here for recorded demo of UIdentify claims intake \(1:05 min\)](#)

FAQ

- Q: Which products within the OPTimum Integrity Cloud are provided as Cloud solutions and which are On-premise solutions?
- A: All products within the OPTimum Integrity Cloud are provided as Cloud solutions. The Cloud model allows On Point to best serve SWA and be most responsive to SWA's needs. The products can also be implemented On-premise or in a Private Cloud infrastructure, if determined to be most valuable for the state. On-premise solutions currently in production for any of On Point's current state customers date back to before states policies allowed for cloud hosted solutions.
- Q: The OPTimum Integrity Cloud infrastructure is stated to FedRAMP moderate certified. What's the current security standard for the OPTimum Integrity Cloud product solutions?
- A: The OPTimum Integrity Cloud is hosted within AWS FedRAMP certified infrastructure. The OPTimum Integrity Cloud product solutions have gone through NIST 800-53 and FISMA audits. We're currently progressing through a 3rd party SOC 2 audit which will be completed by end of February 2021, we'll embark on securing the SOC 2 certification immediately afterwards. On Point is open to participating in any security audits as requested by SWAs during product implementation.
- Q: What's the identity proofing process claimants that do not have an id or submit their claims in paper format?
- A: OPTimum UIdentify does provide an OCR solution where printed copies of a state id can be scanned and processed for validation. This would solve for paper claims. For claimants without a state id, UIdentify can validate other documentation such as utility bills, passports, etc. This is high quality identity verification process but requires more in-dept processes such as scanning integration or manual uploading to scans.
- Q: How do the OPTimum Integrity cloud solutions effectively align with similar products that are already in use by SWA's?
- A: The OPTimum Integrity Cloud utilizes layering of products to strategically block fraud. It does so using different types of systems (physical, systematic, procedural) making it virtually impossible for organized fraud to penetrate. OPTimum Integrity Cloud then employs workload automation layers to process work-items through the integrity stages (prevention, detection, investigation, adjudication, collection, and enforcement). Any solutions currently utilized by SWA's can be integrated within the layering strategy and the OPTimum Integrity Cloud solutions can fill gaps to boost capabilities as deemed valuable. During pre-proposal analysis SWA's and On Point subject matter experts will evaluate any overlap in functionality and determine if including the two systems as layers (for example fraud data analysis would benefit from additional layers of audits) is valuable or if one system would best fit the layer's objective.

