eSAFE™

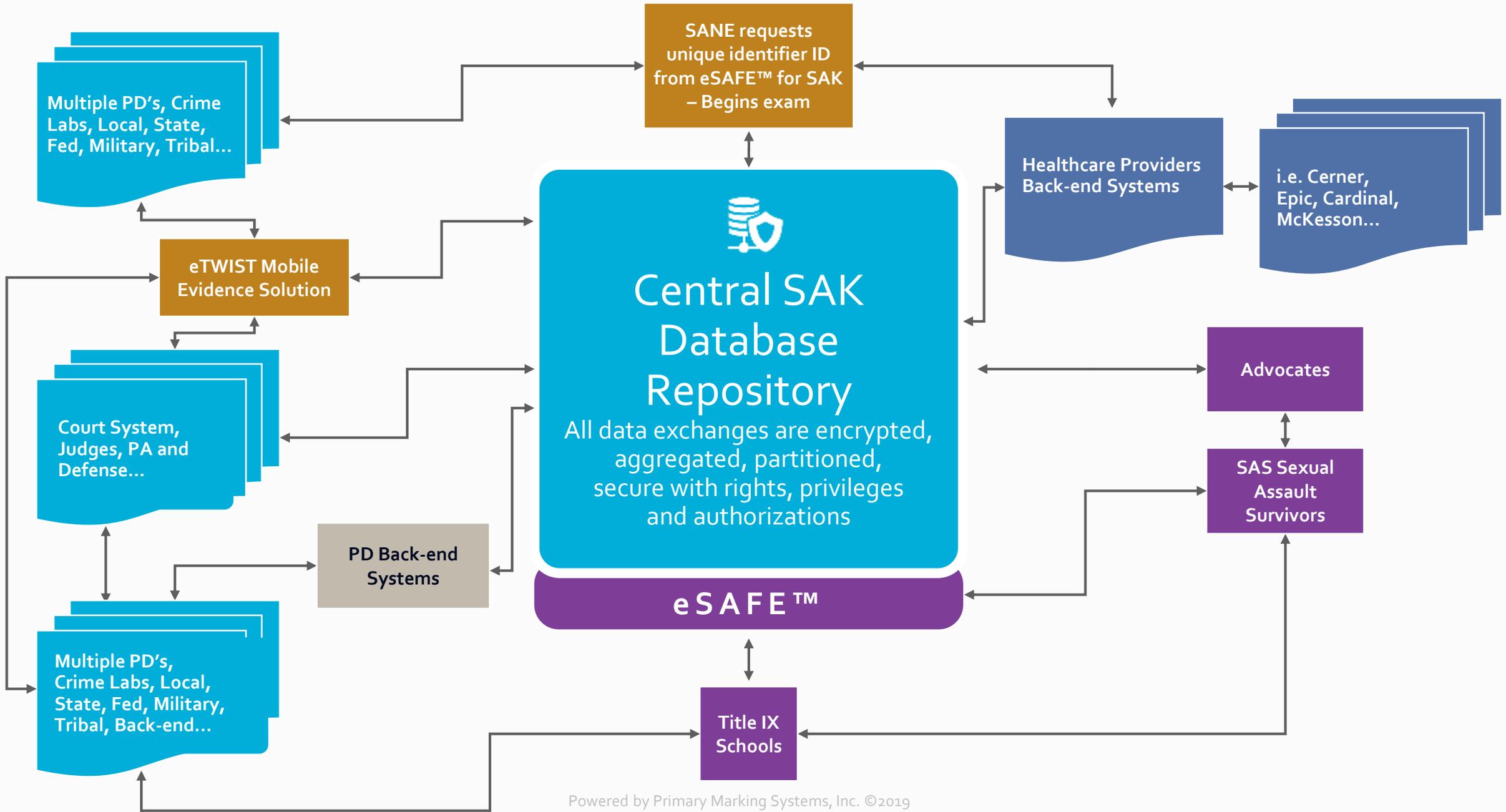**Connecting the Dots**
Tracking technology to unite the justice system and improve prosecution of sexual assault

eSAFE™

Central SAK Database Repository

All data exchanges are encrypted, aggregated, partitioned, secure with rights, privileges and authorizations

eSAFE™

SANE requests unique identifier ID from eSAFE™ for SAK – Begins exam

Multiple PD's, Crime Labs, Local, State, Fed, Military, Tribal...

eTWIST Mobile Evidence Solution

Court System, Judges, PA and Defense...

PD Back-end Systems

Multiple PD's, Crime Labs, Local, State, Fed, Military, Tribal, Back-end...

Healthcare Providers Back-end Systems

i.e. Cerner, Epic, Cardinal, McKesson...

Advocates

SAS Sexual Assault Survivors

Title IX Schools

Powered by Primary Marking Systems, Inc. ©2019

Legislation authorizes new technology
Will it be an asset for prosecutors or simply an administrative headache?

The recent attention directed at the sexual assault kit backlog has led to public demand for change and newfound legislative support. Implementing the wrong system will only lead to more problems.

Technology is needed to improve:

Cooperation

Documentation

Efficiency

Agencies can share information and ideas

Immutable chain of custody

Process works better when everyone is connected

Powered by Primary Marking Systems, Inc. ©2019

Learn from the best

Two decades of evidence and asset tracking expertise in a variety of industries

PMSI is a St. Louis, Missouri based company, founded in 1997. We serve customers as a value-added reseller of data collection and labeling systems accelerating and optimizing cross-business processes throughout the U.S, Europe, and Asia. The company is recognized for its expertise in:

- Software development and deployment
- Mobile computing/Automated data collection
- Thermal Transfer Printers and Supplies
- RFID (Radio Frequency Identification)

We provide exceptional tracking solutions that make it possible for our partners to succeed.

Perhaps you recognize some of our clients:
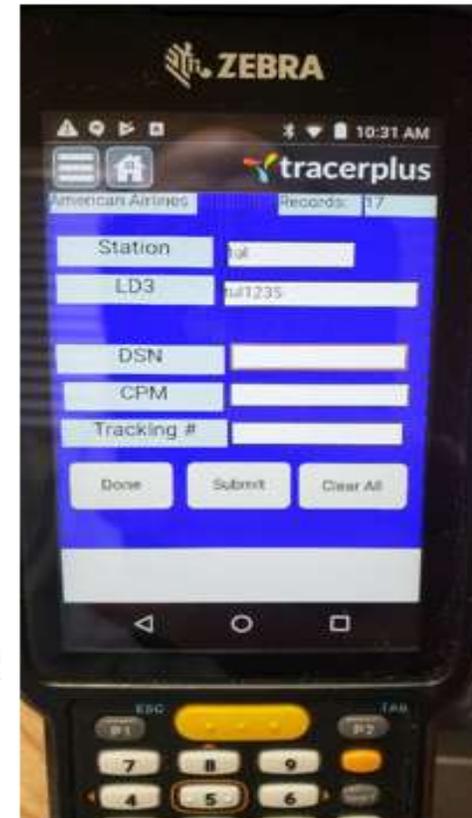
Software package
*Customer: **American Airlines – Processing Maintenance Parts Orders, Tulsa, OK***

Requirement:

The customer desired to record information parts shipments into their current active database. Recording who has completed the work and the items processed. The customer is processing maintenance part orders for airplanes.

Operation:

- The operator enters in the basic information into the handheld unit to identify the location and station doing the work. (Station Code and LD number)
- The operator scans the required 3 fields on the labels. The order sequence of the scans was determined by the customer.
- After the operator scans the 3rd bar code (Tracking Number) the system records the data and restarts the process in field 1 (DSN).
- The handheld unit will sound an audible alarm when the third field is complete.
- The operator continues this process until all items have been scanned.
- Upon completion of the work for the day the operator hits the **Submit** button.
  - Once the **Submit** button is selected, the system stores the information collected into 1 file.
- The information is then wirelessly submitted to the connected database.

The customer will have 8 units in operation in one location. The system greatly enhanced the process by achieving a more accurate audit trail while shortening the time of parts availability.
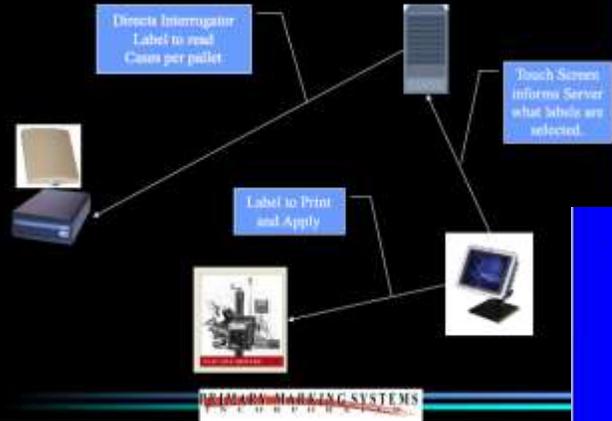
Software package
*Customer: **Prairie Farms Dairy/Walmart RFID- St. Louis, MO***

Software package
*Customer: **Elsevier - St. Louis, MO***

Physical Inventory & Pick Order Routine

Physical Inventory

Enter Employee ID:

`1234`

| Exit | Send Data | Next |

We recommend that the program record an employee id, to capture who collected the data.

Note the green bar in the upper-right corner. This is a battery status indicator which will turn orange as the battery drains and is to alert the user when the device needs to be recharged.

Pick Orders

Scan/Select Order:

`1001` ▼

Scan/Select Item:

`14297392` ▼

Order Qty: **Unit:**

Qty: `2`   **Add**

Loc: `Area A`   **Note**

| Back | Clear | Review | Save |

- The Order can be scanned, entered, or selected from a list. We recommend providing a list to the users, for accuracy. The order number can be retained until all line items are completed.
- The item list will be filtered base on the selected order; that is, the user can only select those items which are line items on the active order. A lookup file will be required.
- If available for lookup, a description, order Qty, and unit of measure or other info can be retrieved from a lookup file and displayed for the user as a visual reference.
- The Add Note button will display a manual entry box to enter a note or comment, if needed.
- The Review button will display a list of the already scanned orders and items, as a reference for the user.

Counted Items

Num	Loc	Count
23100301544	BZ4567	75
57410122345	BZ4567	60
6210000222	BZ4567	22
4578900212	AA1234	27
2800074010	AA1234	25
7431925276	AA1234	50
3700033549	AA1234	20

| Back | Note | | Delete |

- The review screen can contain a delete button to allow the user to delete a record from collected data if needed.

- This screen can also have added a button and field to allow the user to modify a count or quantity if needed.

Avoid common startup mistakes
Our multi-disciplinary team's experience gives you an edge

Primary Marking Systems' guides have the legacy needed to:

Recognize **COMMON PITFALLS**

Offer **SOLID SOLUTIONS** learned from work with a variety of industries

Understand **WHAT'S POSSIBLE** in evidence tracking, asset tracking and system compliance

WATCH FOR LAND MINES as they walk you through the process

Oversimplified systems can destroy a case

Have you thought about how tracking might help you avoid problems with:

MISSING EVIDENCE
Losing a single item such as one document, a component of the sexual assault kit,
a clothing bag, a urine or blood sample sent to a different lab can be disastrous

CHAIN OF CUSTODY
Any unauthorized person handling evidence can destroy a case

IDENTITY ISSUES
- Between departments
- Between states

MISCOMMUNICATION
and lack of information can undermine prosecution and leave victims feeling alienated and vulnerable

Technology exists to prevent these things from happening

LET'S USE IT

1	**Assign unique, non-repeatable identifiers**
2	**Bar code, scan and link all components**
3	**Establish irrefutable chain of custody**
4	**Enable all credentialed stakeholders to track, obtain reports, and receive updates on the status of the kits**
5	**Provide assault survivors or their designee the ability to monitor the status of their kit**

State-of-the-art technology

In February 2019 PMSI was granted their 6th patent for evidence tracking, 2 additional SAK patents pending

Cutting edge technology increases security

PMSI's technology partners assure that:

1	2	3	4
Mobility coupling Block Chain technology recording a solid audit trail for chain of custody	HIPPA, HPI, PPI, and other compliance regulations can be met	Only stakeholders with documented authorization will have access	Auditing becomes much easier when 1-3 are done correctly

Powered by Primary Marking Systems, Inc. ©2019

Built-in compliance

Compliance	Supporting	Data Centers Tested	Foundational Standard	@ TierPoint Facility Level	@ Client Deployment Level
SOC 1 – Type 1	*Foundational audit showcasing corporate controls and financials*	All	●	●	●
SOC 1 – Type 2	*Foundational audit showcasing foundational controls and security*	All	●	●	●
PCI-DSS – Colocation	*Payment Card Industry – Now testing all 12 sections*	All	●	●	●
HIPAA	*Health and Patient protection*	All	●	●	●
NIST 800-53	*Foundational Audits for Internal Security Controls*	All	●	●	●
GLBA	*Insurance & banking regulation to maintain separation of infrastructure*	All	●		●
HI-TRUST	*New Health and Patient audits to be completed in 2019*	All	●		●
NERC	*Specific Compliance for nuclear regulatory infrastructures*	3			●
FISCAM*	*Baseline to bridge NIST-800 + specific audit layers for state, fed gov'ts*	3			●
PCI-DSS – Cloud	*Managed cloud infrastructure*	2*		●	●
IRS-PUB 1075	*Department of Revenue security mandate – State of South Carolina*	2	●	●	●
FISMA	*Expansion of Government sales capabilities*	2*		●	●

TierPoint has expanded our compliance certifications 300% since 2015.

**Will expand this testing to other data centers in 2019*

Built-in Security: Details

Service	Notes	Colocation	Managed Hosting	Multitenant Cloud	Hosted Private Cloud
Data Center Compliance Controls*	*Compliance layer mapped across all facilities*	●	●		●
Physical Security Controls	*Includes gates, biometrics, badges, secure cages, etc.*	●	●	●	●
Foundational DDoS	*Protection against volumetric and non-volumetric attacks*	●	●	●	●
Credential Management	*CyberArk and A/D integrations for least privileged access controls*	●	●	●	●
SSL Portal Access	*Secure access to view and manage environments*	●	●	●	●
Net Flow analysis with A.I. programs	*Better understanding of BOT traffic and zero trust profiles*		●	●	●
Network VLAN Segmentation	*Creates collection of isolated networks within data center*		●	●	●
Security applied to higher disciplines	*FISMA, PCI, HIPAA, HI TRUST, IRS-PUB 1075, NIST-800-53*		●	●	●
Hypervisor Patch Management	*Managed updates to infrastructure hypervisors*			●	●
Encrypted Storage	*Data encrypted at rest on storage media*			●	●

■ Perimeter   ■ Core & Edge Networks   ■ Hosts & Users   ■ Apps & Data

These controls are one element in a larger set of compliance requirements that clients will need to consider based on their individual circumstances.

Built-in: By the numbers

Client Audit Support

- The TierPoint information Security Office supports over 1800 individual client audits per year to help clients maintain PCI, HIPAA and their own SOC 2 complicacies.

Compliance Mandates for Clients

- The TierPoint Information Security Office supports over 1200 clients with our SOC 2 and PCI audit report distributions. These clients represent an MRR of $17,989,182 or $215,870,189 in yearly revenue.

Internal DDoS protection

- External DDoS attacks mitigated by our built in Radware infrastructure in 2018: 1,266,996

  - Infrastructure attacks: 680,733

  - Customer Attacks: 589,072

- External WAF attacks mitigated by our built in Radware infrastructure in 2018: 2,215,529

  - TierPoint.com: 917,926

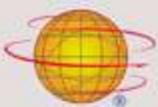 - BraveIT.Tierpoint.com: 274,123

  - Client & Other: 1,023,480

**Voice Authentication &
Legally-Binding
*Voice Signatures***
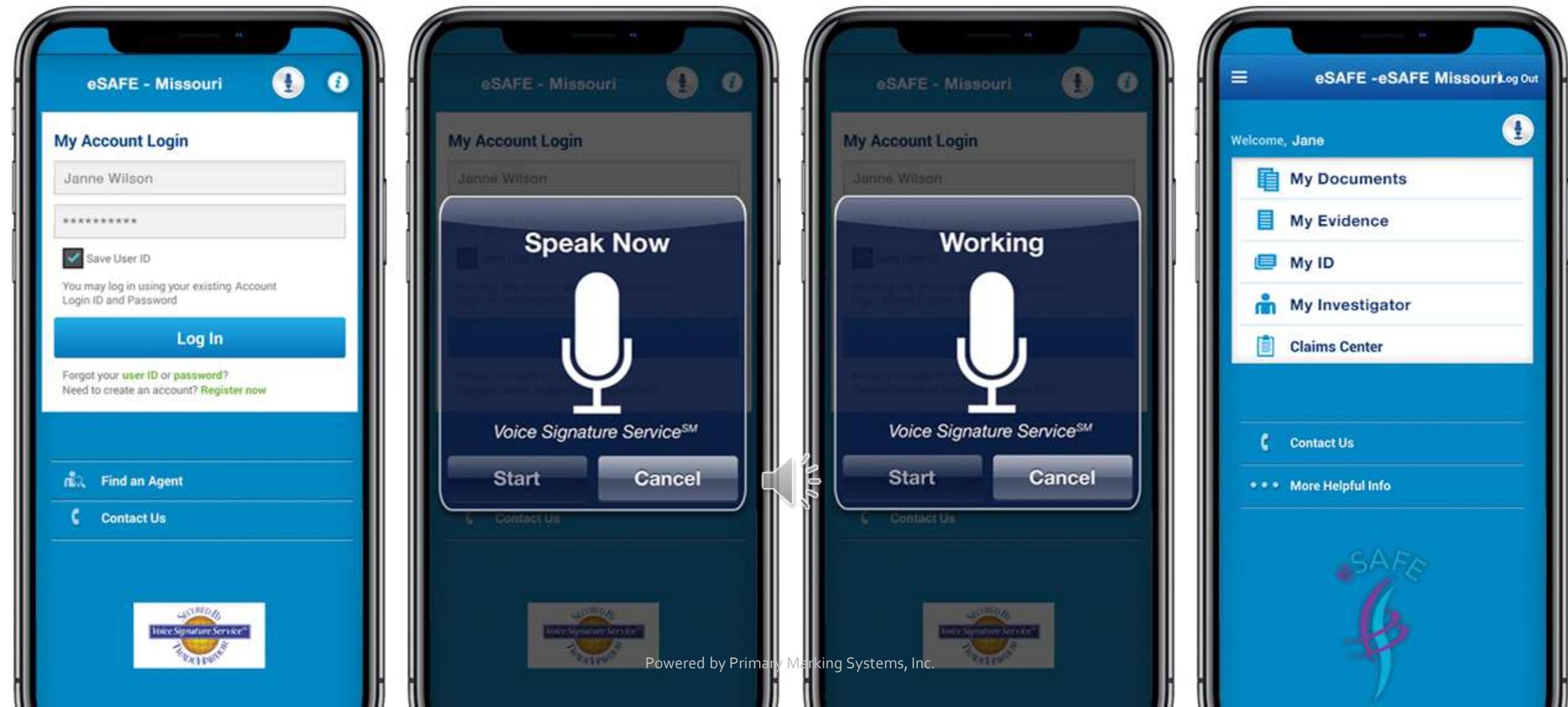
TRADEHARBOR® *The Voice Signature Company*

Customers

Commonwealth of Virginia · UNUM · COSTCO WHOLESALE · rivetz · CYBER DEADBOLT · Genesys · INTERACTIVE INTELLIGENCE · RELIANT CONSULTING · EGroup Business Loans · YoungWilliams

Department of ELDER AFFAIRS STATE OF FLORIDA · FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES MyFLFamilies.com · Kansas City · ibu Interviews by Underwriters · The FutureWorks Group · USDA · CMS CENTERS FOR MEDICARE & MEDICAID SERVICES · IRS · Banamex · RPC An Oil & Gas Services Company

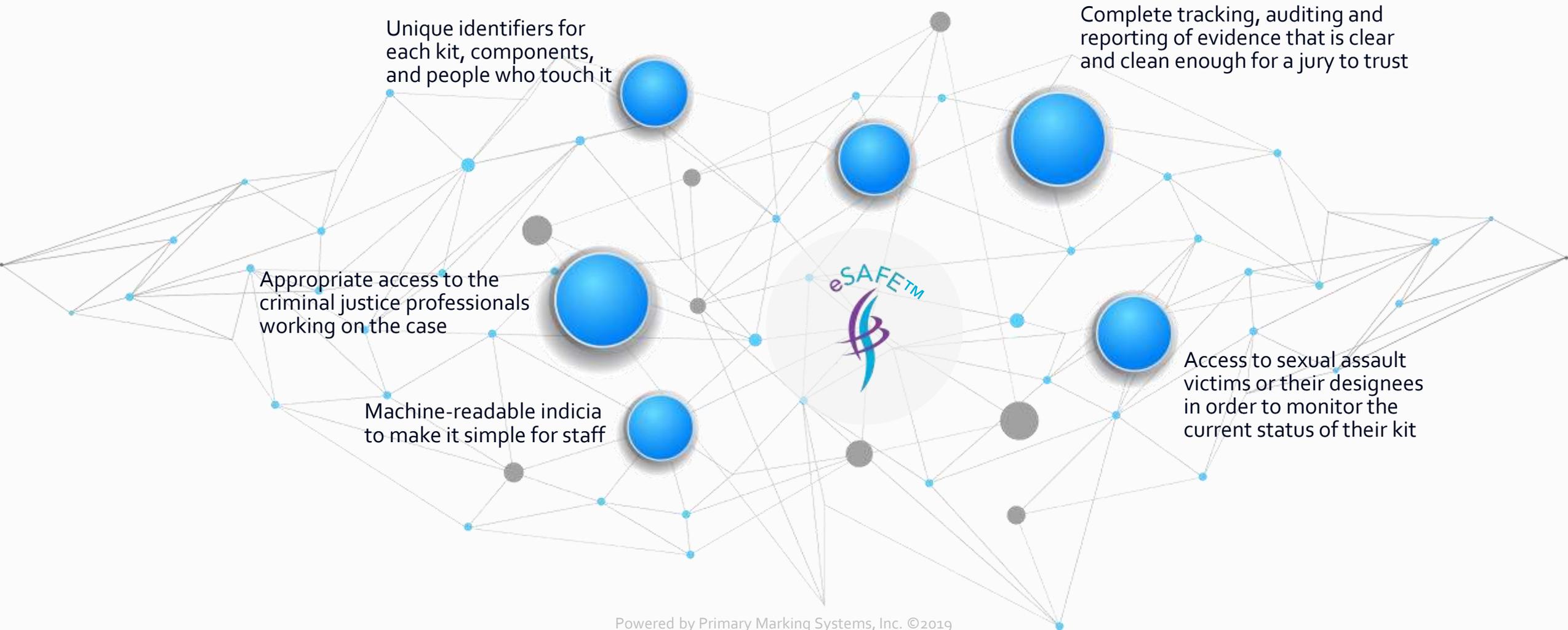MetLife · citi · PAYCHEX · NAVIENT Solutions for your success · Morgan Stanley · TEXTRON · FirstEnergy · Enterprise Products Partners L.P. · Kroger · Bank of America

This isn't about putting a sticker on a box
It's about connecting the dots so a jury will convict

Unique identifiers for each kit, components, and people who touch it

Complete tracking, auditing and reporting of evidence that is clear and clean enough for a jury to trust

Appropriate access to the criminal justice professionals working on the case

eSAFE™

Machine-readable indicia to make it simple for staff

Access to sexual assault victims or their designees in order to monitor the current status of their kit

Central SAK Database Repository

All data exchanges are encrypted, aggregated, partitioned, secure with rights, privileges and authorizations

eSAFE™

SANE requests unique identifier ID from eSAFE™ for SAK – Begins exam

Multiple PD's, Crime Labs, Local, State, Fed, Military, Tribal...

eTWIST Mobile Evidence Solution

Court System, Judges, PA and Defense...

PD Back-end Systems

Multiple PD's, Crime Labs, Local, State, Fed, Military, Tribal, Back-end...

Healthcare Providers Back-end Systems

i.e. Cerner, Epic, Cardinal, McKesson...

Advocates

SAS Sexual Assault Survivors

Title IX Schools

Powered by Primary Marking Systems, Inc. ©2019

Tracking sexual assault kits
provides significant benefits to states and citizens

1   811 serial rapists identified from testing backlogged kits in Detroit[1]

2   82% of victim-identified rape suspects in Kansas committed additional violent crimes[2]

3   1/3 of rape suspects in Ohio assaulted someone who knew them, as well as strangers assaults[3]

4 $1,641 to test a rape kit can avert sexual assaults costing an average of $133,500[4]

5   Front end investment pays the biggest dividend for public safety[5]

[1] Wayne County Sexual Assault Kit Task Force FAQ, Sept. 2017
[2] Kansas Bureau of Investigation Sept. 2017
[3] Begun Center for Violence Prevention at Case Western Research University
[4] *March 2018 study by Stanford*
[5] *2017 Missouri State Justice Task Force*

The stakes are too high to go with a solution that doesn't improve prosecution

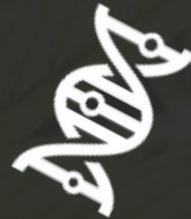# Proven steps for successful implementation of proven technologies

Visioning & Alignment
Proof of concept

Design
Initial operating capabilities

Deploy
Full operating capacity

Implement
Final acceptance and full rollout

eSAFE™

Is available on the NASPO ValuePoint Master Price Agreement number MNWNC-130

A well-planned system

CONTRACTS

DNA
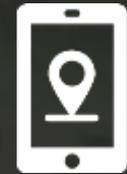
eSAFE™

Mobile Evidence Tracking

Legalized marijuana

Powered by Primary Marking Systems, Inc. ©2019

We can help you make Missouri a safer place

THANK YOU

eSAFE™

Primary Marking Systems, Inc.

Tim McIntyre, *VP Government Solutions*
316 Jungermann Road
St. Peters, MO 63376
(314) 344-9178 ext. 202

✉ tmcintyre@primarymarking.com