



**SERS Retirement Board
Technology Committee Meeting
June 20, 2024
1:30 P.M.**

Join Zoom Meeting

<https://ohsers.zoom.us/j/96697005169?pwd=dEd6STZaS2RlOSs1NWwrT09MWW5CZz09>

Meeting ID: 966 9700 5169 **Password:** 12345

To join by phone, dial: +1 305 224 1968 and enter the Meeting ID: **966 9700 5169** and Password: **12345** when prompted.

1. Roll call
2. Approval of **April 18, 2024**, Technology Committee Minutes (R)
3. Opening Remarks
4. Information Technology Update
 - Education Session Under R.C. 171.50 and 3309.051 – Cybersecurity
 - Technology Committee Updates
 - Technology Roadmap (TRM) Infrastructure and SMART
 - TRM Financial Tracking
 - Risk Management Q4
5. Risk Management and Information Security Quarterly Update
6. Executive Session pursuant to R.C. 121.22(G)(6) to discuss a security matter (*if needed*)
7. Upcoming Technology Committee Meetings
 - Future Topics
 - Next Meeting Date(s)
8. Adjournment

**SERS Special
Technology
Committee Meeting
June 20, 2024**

_____ P.M.

Roll Call:

Matthew King	_____
James Rossler	_____
Frank Weglarz	_____
Daniel Wilson	_____

**APPROVAL OF MINUTES OF THE TECHNOLOGY COMMITTEE MEETING HELD ON
April 18, 2024**

_____ moved and _____ seconded the motion to approve the minutes of the Technology Committee meeting held on **April 18, 2024**.

Upon roll call, the vote was as follows:

<u>ROLL CALL:</u>	<u>YEA</u>	<u>NAY</u>	<u>ABSTAIN</u>
Matthew King	_____	_____	_____
James Rossler	_____	_____	_____
Frank Weglarz	_____	_____	_____
Daniel Wilson	_____	_____	_____

<p>School Employees Retirement System</p>	<p align="center">TECHNOLOGY COMMITTEE MINUTES</p>		
<p>Preparer</p>	<p>Megan Robertson</p>	<p>Meeting Date:</p>	<p>April 18, 2024</p>
<p>Committee Chair</p>	<p>Matthew King</p>	<p>Committee roll call was as follows: Matthew King, James Rossler, Frank Weglarz, Daniel Wilson</p> <p>Also in Attendance: SERS Staff Members: Phil Grim, Jay Patel, John Grumney, Jeff Davis, Joe Marotta, Richard Stensrud, Karen Roggenkamp, Vatina Gray, Nikki Whitacre, Laura Troiano, and Megan Robertson. The representative of the Ohio Attorney General, Lisa Reid and guests attended virtually on Zoom.</p>	
<p>Agenda</p>	<ol style="list-style-type: none"> 1. Roll call (R) 2. Approval of December 21, 2023, minutes (R) 3. Opening Remarks 4. Information Technology Update <ul style="list-style-type: none"> o Technology Roadmap – Infrastructure and SMART o Telecomm/Contact Center Conversion (UCaaS/CCaaS) o Member Services Upcoming Projects o Technology Roadmap Financial Tracking 5. Risk Management and Information Security Quarterly Update <ul style="list-style-type: none"> o School Cyber Incident Notification SERS o FY2025 Budget 6. Executive Session pursuant to R.C. 121.22(G)(6) to discuss a security matter (<i>if needed</i>) 7. Upcoming Technology Committee Meetings <ul style="list-style-type: none"> o Future Topics o Next meeting Date(s) 8. Adjournment 		
<p>Discussion</p>	<p>The SERS Special Technology Committee meeting began in open session at 1:18 p.m.</p> <p><u>Roll Call</u></p> <p>The SERS regular Technology Committee began with a roll call. The committee roll call was as follows: Present: James Rossler, Frank Weglarz, Daniel Wilson, Matthew King.</p> <p>Also in attendance were SERS Staff Members: Phil Grim, Jay Patel, John Grumney, Jeff Davis, Joe Marotta, Richard Stensrud, Karen Roggenkamp, Vatina Gray, Nikki Whitacre, Laura Troiano, and Megan Robertson. The representative of the Ohio Attorney General, Lisa Reid, and guests attended virtually on Zoom.</p> <p><u>Approval of Minutes</u></p> <p>Jamie Rossler moved, and Frank Weglarz seconded the motion to approve the minutes of the Technology Committee meeting held on December 21, 2023. Upon roll call, the vote was as follows: Yea: Matthew King, James Rossler, Frank Weglarz, Daniel Wilson. The motion carried.</p> <p><u>Information Technology Update</u></p>		

SERS Deputy Executive Director, Karen Roggenkamp briefly highlighted features of the recent Telecomm platform conversion, explaining it has introduced beneficial features for the organization, particularly the Member Services contact center. Ms. Roggenkamp shared that the Committee would get a better understanding of the benefits it offers for member support through today's presentation.

Jay Patel, SERS Chief Technology Officer, shared a Technology Roadmap update on FY2024 Infrastructure projects and FY2024 SMART projects, beginning with the UCaaS/CCaaS project which replaces end of life phone system. Mr. Patel elaborated on the significant accomplishment of taking the existing telecom system, which was approximately twenty years old, and moving to the new cloud-based phone system with disaster recovery and service continuity capabilities. . The new system was rolled out on March 27, 2024, and continued over the next three weeks. Mr. Patel continued his update on additional projects. Plans are being formed to replace Palo Alto Firewalls. After an evaluation CrowdStrike was retained for end-point protection as a part of the Information Security project. Several other security projects are under evaluation and review. In terms of data resilience and protection, several initiatives are planned for fiscal FY2025.

Mr. Patel shared images of SERS on the premises Avayla infrastructure with the committee. The committee received insight as to what it took to run the old telecom platform which was reaching its end of life and going away. To close his update on the phone system project, Mr. Patel briefly covered some key benefits from the implementation of UCaaS/CCaaS with the committee. Mr. Patel explained this is a technology that gets us closer to the vision of enhanced customer service. Mr. Patel recognized before the committee many SERS staff members by name who played a key role in the completion of this project, helping bring it to fruition. Mr. Patel explained the appropriate use of SERS phone tools, Zoom phone for external communication and Teams for internal communication. Mr. Patel elaborated that with these two options SERS has flexibility and enhanced disaster recovery options.

Mr. Patel introduced John Grumney, Director of Member Services, to the committee to elaborate on the positive enhancements the new phone system offers for the Member Support Team (MST) in Member Services. Mr. Grumney thanked the committee for their support with the new phone system. Mr. Grumney provided a brief background on the history of the MST model and the MST leadership. Mr. Grumney elaborated on the nature of the calls received and shared MST's recent stats and positive survey results. Mr. Grumney elaborated on a new key feature of call waiting offered through the new phone system. This feature ensures members will receive a return call at the soonest availability without waiting on the phone or losing their place in line. Mr. Grumney shared an example of the MST Dashboard with the committee. The Dashboard shows how calls are handled and the excellent self-management tools it provides to the team. Mr. Grumney explained another brand-new feature with the phone system allows a manager to join a call live and speak to the representative assisting a customer without the customer being interrupted. Mr. Grumney explained this tool is great for training and side by side coaching. Mr. Grumney continued his report, sharing additional artificial intelligence (AI) utilization with the phone system is all internally focused to help staff in managing the calls and voicemails ultimately improving staff development and self-awareness.

Among other conversion benefits, SERS had a handful of cell phones among staff but now in the Cloud those cell phones are not needed anymore. The plans were cancelled, allowing cost reduction. Additionally, with the call back feature in place SERS anticipates future cost reduction in the phone bill.

	<p>After a few questions from the Board and a brief discussion surrounding the new phone system the committee moved on with the updates.</p> <p>Mr. Patel continued his update on FY2024 SMART projects, elaborating on the upcoming Member Self Service portal registration reimagination project to improve multi-factor authorization and user experience.</p> <p>Mr. Patel provided an update on the Technology Roadmap Budget. As shared previously with the committee, some initiatives may get pushed to FY2025, but otherwise the technology roadmap is under budget and tracking through the FY2024 plan.</p> <p><u>Risk Management and Information Security Update</u></p> <p>Ms. Roggenkamp introduced Information Security Officer, Phil Grim to the committee to cover the risk management and information security updates.</p> <p>Mr. Grim provided an update on School Cyber Incident Notification to SERS. The Ohio Administrative Code language was proposed to the full board by Legal in the regular April 2024 board meeting. Next it will go before JCARR for review and approval, and finally will go back before the SERS Board for final approval. Mr. Grim continued his updates, covering an Information Security Enhancements in FY2025 Budget Request and FY2025 Staffing Budget Request.</p> <p>Mr. Grim continued his report by providing the key metrics on Information Security's three lines of defense: Proofpoint, Microsoft, and Staff. After questions from the committee and a brief discussion, Mr. Grim continued his report on inbound email and blocked messages.</p> <p><u>Upcoming Technology Committee Meetings – Future Topics and Next Meeting Dates</u></p> <p>Matt King and other committee members requested an executive session to be held at the June meeting providing more details on the online refund processing project with Socure.</p> <p>The next regular Technology Committee meeting will be held Thursday, June 20, 2024, at 1:30 pm or immediately following the regular SERS Board Meeting.</p> <p>Technology Committee Chair, Matthew King, adjourned the meeting at 2:03 p.m.</p>		
	Action Items	Assigned Person	Due Date
Action Items	n/a		

Matthew King, Committee Chair

Richard Stensrud, Secretary



TECHNOLOGY COMMITTEE

June 20, 2024

Agenda Items



- **Opening Remarks**
- **Educational Session: Cybersecurity**
 - Identity Proofing Accounts
 - Combating Email Threats
- **Technology Committee Updates**
 - Technology Roadmap (TRM) – Infrastructure and SMART
 - TRM Financial Tracking
 - Risk Management Q4
- **Questions/Future Topics**



Identity Proofing Accounts

Introduction



Key Takeaways

- Fraud is a real concern.
- There are various types of fraud, but we will focus on those that present the greatest risk to members and online presence.
- Artificial Intelligence will become an integral part of the future (good and bad).
- The dark web is a trove of information that creates risk to organizations and people.
- Identity Proofing is challenging and required.
- Email will remain a valuable tool and it must be monitored through more than one lens.

Identity Proofing Accounts



Fraud is defined as a wrongful or criminal deception intended to result in financial or personal gain, and can be committed internally or externally by employers, employees, third-party vendors, or others.



Fraudsters were able to obtain sufficient information about a true beneficiary to convince the Social Security Administration that they were that beneficiary. Once they were in the front door, they were able to change their direct deposits.



- Jeffrey Brown

Deputy Assistant Inspector General, Office of the Inspector General

Types of Fraud



Internal Fraud

Able to commit fraud because there is:

Opportunity

Inadequate internal controls

Pressure

Personal financial issues or vices/additions

Rationalization

Justification for actions

External Fraud

First-Party Fraud

Fraud committed against an organization to gain a benefit they were not entitled to otherwise

Uses synthetic identity

Bust-out fraud,
Chargeback fraud,
Fronting, Goods Lost in Transit Fraud, De-shopping, Government loan fraud

Second-Party Fraud

When an individual knowingly gives their identity or personal information to another person, to commit fraud.

Money muling

Third-Party Fraud

Victim Fraud

When someone commits a fraudulent action against an individual

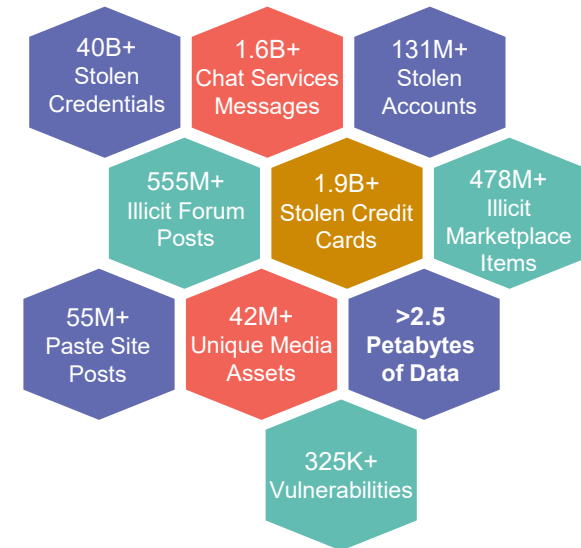
Familiar Fraud

Friend or family that takes advantage of access to the victim

Identity Proofing Accounts



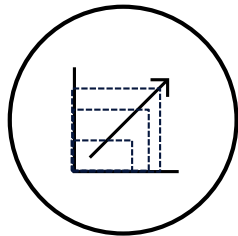
Identity Proofing Accounts



“Threat Actors” are accelerating

Source: Flashpoint

Identity Proofing Accounts



Scale Attacks



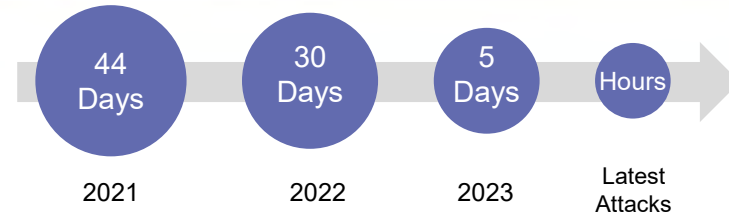
Execute hundreds of simultaneous attacks

(Solarwinds with precision vs. random network targeting)



Exploit several vulnerabilities

Accelerated identification of external exposures and scale the attacks



Date	Product	Vulnerabilities	Exposed Devices
Jan 5, 2023	Sugar CRM	CVE-2023-22952	5,696
May 31, 2023	MOVEit	CVE-2023-34362 CVE-2023-35036 CVE-2023-35708	2,043
July 18, 2023	Citrix RCE	CVE-2023-3519	48,279
July 24, 2023	Ivanti MobileIron	CVE-2023-35078	5,033

Identity Proofing Accounts



Impact of MOVEit attack across pension funds:

- Tennessee Consolidated Retirement System
- California Public Employees Retirement System
- California State Teachers' Retirement System
- Central States Pension Fund
- Virginia Retirement System
- New Hampshire Retirement System
- Employee Retirement System of Rhode Island
- Teachers Retirement System of Georgia
- Teachers Insurance and Annuity Association of America (domino effect across 15,000 institutional clients)
- Teachers' Retirement System of the City of New York
- 457 colleges and universities



First Name, Last Name, Social Security Number, Date of Birth, Address

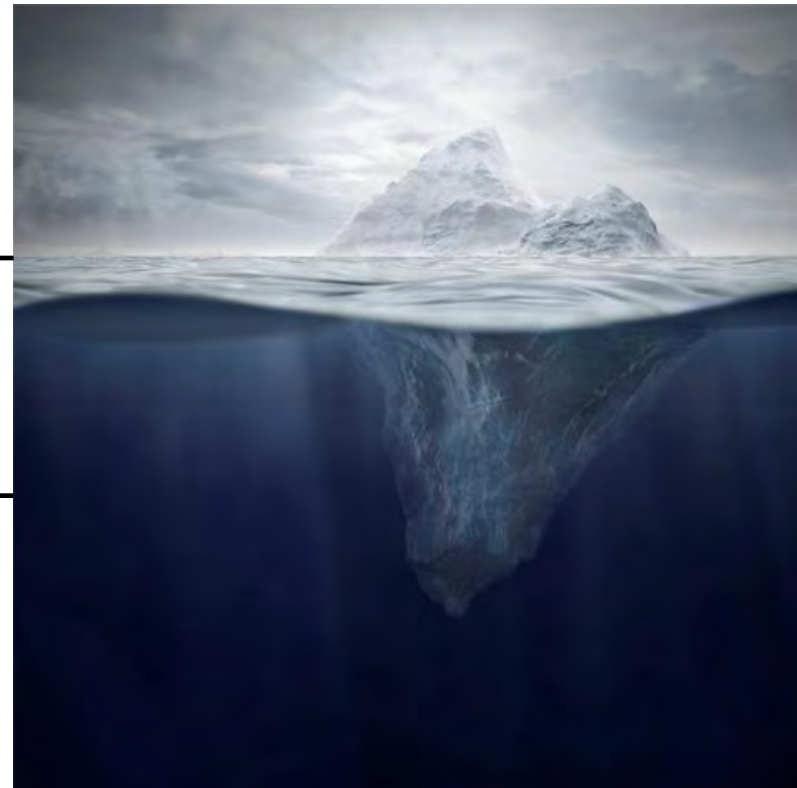
Identity Proofing Accounts



5% **Surface web** – includes publicly visible websites (blogs, shopping sites, news sites, YouTube)

90% **Deep web** – consists of sites that require a login to access (email accounts, banking portals, subscription services)

5% **Dark web** – is the part of the deep web that isn't indexed by search engines and requires special tools to access, like TOR browser



Identity Proofing Accounts – Stealer Logs



Harvested Email Accounts (sample)

xxxxxxxxxyyy@gmail.com
xxxxxxxxxyyy@gmail.com
xxxx.xxxx@gmail.com
xxxxxx_xxxxxxx@icloud.com
xxxxxxxxxyyy@gmail.com
xxxxxy_xxxx@yahoo.com
xyyyyyy@outlook.com
xxxxxxxxxyyy@gmail.com
xyxxxxx@gmail.com
xxxxxxxxxy@proton.me
xxxxxxxxxy@att.net

Harvested Accounts & Passwords (sample)

Host: | Username: xxxxx_xy | Password: jmp*****
Host: | Username: xxxxx_xxxxxx@icloud.com | Password: Jmp*****
Host: | Username: xxxxxxxxxxxxyyy@gmail.com | Password: jmp*****
Host: | Username: xxxxxxxxxxxxxxxx@gmail.com | Password: jmp*****
Host: | Username: xxxxxxxxxxxxy@gmail.com | Password: Hyp*****

Harvested Websites Visited (sample)

Host: https://mortgage-application.net/myaccount/ | Username: xxxxxxxx
Host: https://account.proton.me/ | Username: xxxxy@proton.me | Password: Cp:****
Host: https://accountaccess.myfedloan.org/ | Username: xxxxy | Password: Hyp*****
Host: https://accounts.google.com/signin/ | Username: xx@gmail.com | Password: Jmp***
Host: https://accounts.intuit.com/index.html | Username: xxxxx | Password: Hyp*****
Host: https://identity.doordash.com/ | Username: xxxxx@gmail.com | Password: Jmp**
Host: https://leasing.stellantis-fs.com/ | Username: xxxxx@gmail.com | Password: Hyp***
Host: https://login.teamviewer.com/ | Username: xxxxx@gmail.com | Password: Jmp***
Host: https://myaccount.gmfinancial.com/login | Username: xxxxx | Password: Ver*****
Host: https://personal.vanguard.com/us/ | Username: xxxxx | Password: Ver*****
Host: https://ring.com/users/sign_in | Username: xxxxx@gmail.com | Password: Jmp***
Host: https://secure.chase.com/auth/logonbox | Username: xxxxx | Password: Hyp***
Host: https://twitter.com/i/flow/login | Username: xxxxx | Password: jmp*****
Host: https://www.aepohio.com/ | Username: xxx@gmail.com | Password: jmp*****
Host: https://www.amazon.com/ap/signin | Username: xxxx | Password: jmp*****
Host: https://www.ebay.com/signin/ | Username: xxx@gmail.com | Password: jmp***
Host: https://www.facebook.com/login/ | Username: xxx@icloud.com | Password: jmp**
Host: https://www.gmfinancial.com/myaccount/ | Username: xxx@gmail.com | Password:
Host: https://www.hulu.com/welcome | Username: xxx@gmail.com | Password: Hyp***
Host: https://www.ihg.com/hotels/reservation | Username: xx@yahoo.com | Password: 718*
Host: https://www.xhealth.com/my-account/ | Username: xx@gmail.com | Password: Hyp***
Host: https://www.mycard.mobi/login/ | Username: xxxx | Password: Ver****
Host: https://www.zillow.com | Username: xxxx | Password: Jmp*****

Dark web (Stealer Logs) Sold: \$20

Identity Proofing Accounts



Additional examples of risks:

- AI-generated Spear-Phishing Emails
 - Targeting the organization
 - **Targeting the customer**
- AI-generated Cyber Attacks
 - Can be created in less than 24 hours and scaled rapidly
- Generated Deepfake Video and Audio Files
 - Spread false information
- Generated Images
 - **Accelerate the creation of fake ID documents**
- Generated Text
 - Phishing and SMiShing content
 - Sophisticated chatbots on social networks
- Generated Audio
 - Voice cloning as-a-service
 - Business fraud through wire transfer calls
- Synthesized Identity Data
 - Generate fictitious identities
- AI-Automated Fraud
 - Vulnerability scanning
 - Intelligent detection and exploitation of system weakness
 - Development of adaptive malware
 - **Identity and credential theft, or account takeover**

Identity Proofing Accounts



Web application firewalls are not enough

- Web application firewalls and bot detection at the network layer does not work completely
- Only targets high frequency IP's and obvious fraud
- Easily beat by masking user-agent, rotating IP, using cell phone networks

reCAPTCHA

- High false-positives when coming from a corporate/VPN network
- Google v3 and v2 reCAPTCHA is easily beatable by GenAI and emulation
- Google v2 has accessibility issues

Block Email Domains

- Blocking temporary email domains and specific domains will work at first but can lead to high false positives
- Fraud will eventually migrate to domains that can't be blocked (Gmail, Hotmail, Yahoo, AOL, Outlook)

Identity Providers (IDP) can't help

- Identity Provider's focus on authentication and risk after an account has been created
- Open citizen account creation normally goes unprotected

The old way of thinking does not work.

Identity Proofing Accounts



SP 800-63 Digital Identity Guidelines

Identity Assurance Levels

- **IAL1:** Identity claims are self-asserted and not linked to a specific real-life individual.
- **IAL2:** Evidence supports the real-world existence of the claimed identity and establishes the applicant as the true owner of this identity.
- **IAL3:** Identity proofing is supervised by an authorized representative with specialized hardware if appearing remotely.

Financial Services: Banks, investment firms, and fintech companies implement NIST IAL2 to secure online banking, investment accounts, and financial transactions.

Healthcare: healthcare providers secure patient information with NIST IAL2 for accessing electronic health records (EHRs) and other confidential data.

Government Services: Government agencies employ NIST IAL2 to safeguard citizens' personal information and ensure secure access to services like tax filing, social security, and immigration services.

E-commerce and Retail: Online retailers use NIST IAL2 to enhance security during payment processing and protect user accounts from unauthorized access.

Telecommunications: Telecom companies employ NIST IAL2 to secure customer information, especially for services that involve sensitive data like call records and billing information.

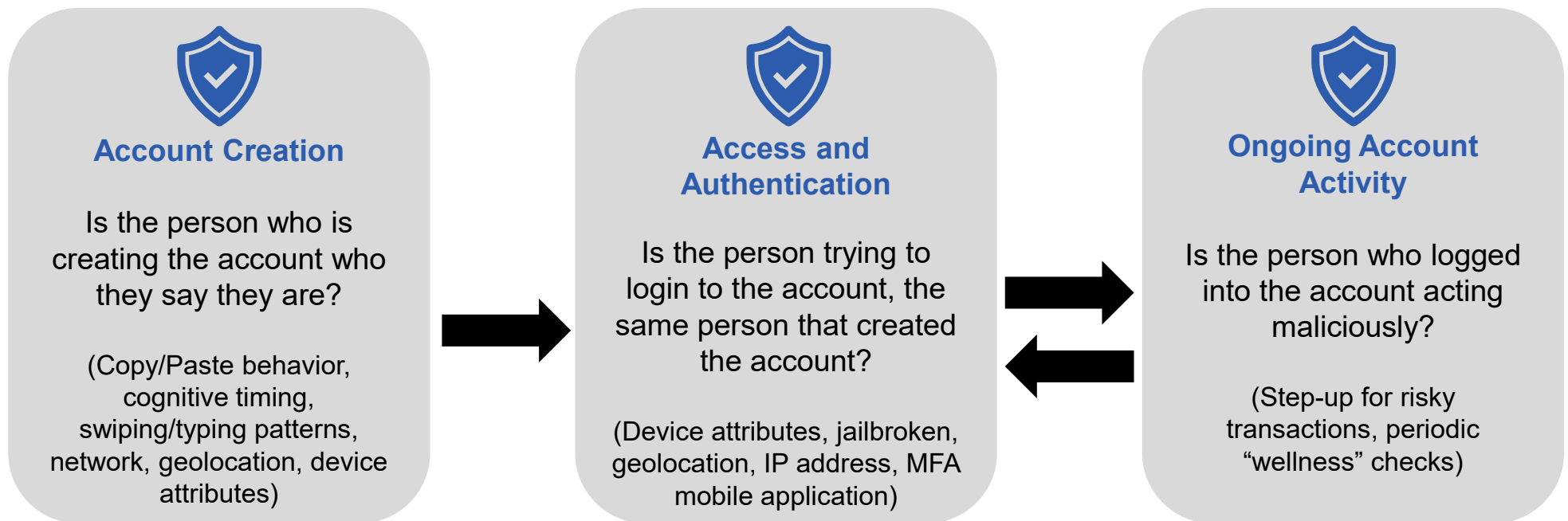
Education: Educational institutions implement NIST IAL2 to secure access to student records, online learning platforms, and other sensitive academic data.

Knowledge-Based Authentication, referred to as “security questions”, is no longer recognized as an acceptable authenticator by SP 800-63-3 (June 2017).

Identity Proofing Accounts



Summarized as having three main components:



Identity Proofing Accounts



2,200+

Customers across financial services, telecom, gaming, ecommerce, public sector:

- 14 of 15 Top Banks
- 13 of 15 Top Credit Card Issuers
- 4 of 5 Top MSBs
- 400+ Largest Fintechs
- Largest Payroll Service
- Largest Prepaid Issuer
- 3 of Top 4 Gaming Operators
- 4 of 4 Largest States



AI/ML is in their DNA

Data Science & Engineering is over 40% of the company's headcount

\$353M in private venture funding

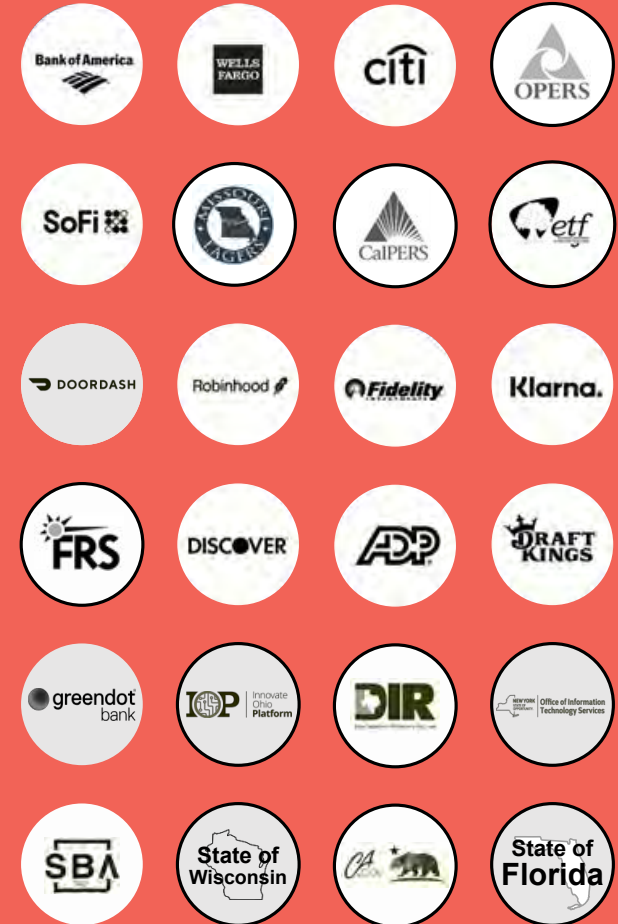
Accel, Scale Ventures, Commerce, Capital One, Citi, Wells Fargo, T. Rowe

Remote-First Team

Regional offices in U.S. 400 employees














379%

ARR Growth: 2019 to 2023



Identity Proofing Accounts



POWERFUL GRAPH-DEFINED FRAUD PREVENTION			DATA-DRIVEN REGULATORY COMPLIANCE	INSTANT DOCUMENT VERIFICATION
 <p>Sigma Identity Fraud Every dimension of consumer identity is analyzed to detect third-party fraud across the digital lifecycle</p>	 <p>Digital Intelligence Combined device intelligence, behavioral analytics, and entity profiling associate device, behavioral, network, and location patterns at scale</p>		 <p>Socure Verify Verifies first name, last name, address, phone, DOB, SSN correlation for precise identity resolution of nearly any consumer</p>	 <p>Predictive Document Verification Instant ID document with ML models and biometric verification with NIST PAD Level 2 liveness detection</p>
 <p>Sigma Synthetic Fraud Purpose-built module combines proof-of-life data sources and advanced ML trained on synthetic- specific features</p>	 <p>First-Party Fraud Consortium ML model detects fraud where true identity is asserted, for abuse, bust out, friendly fraud, and no intent to pay</p>	 <p>Alert List Socure's consortium database of known harmful identities weeds out bad actors</p>	 <p>Global Watchlist Screening with Monitoring Hyper-accurate sanctions and risk screening with continuous customer status monitoring ensures uninterrupted compliance</p>	
 <p>Email RiskScore ML model trained on hundreds of email-specific variables and data sources, correlated to an identity</p>	 <p>Phone RiskScore ML model trained on hundreds of phone-specific variables and data sources, correlated to an identity</p>	 <p>Address RiskScore ML model trained on hundreds of address-specific variables and data sources, correlated to an identity</p>	 <p>eCBSV Instantly verify a consumer provided name, SSN and DOB match with the issuing authority</p>	<p>ACCOUNT INTELLIGENCE</p>  <p>Account Intelligence Instant, inclusive bank account status and ownership verification</p>



DECISION MODULE

Hosted controls interface that orchestrates customer decision logic

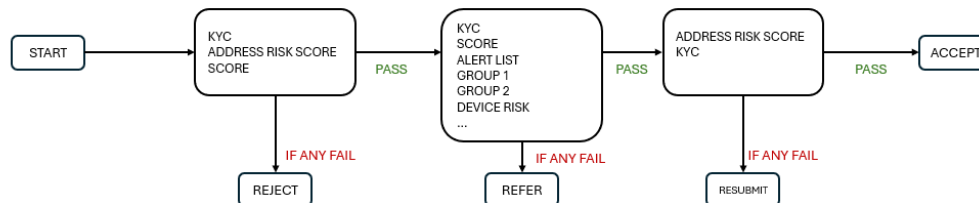
Identity Proofing Accounts



Workflow features

- No programming required
 - Configuration, not customization
- Drag-and-Drop
- Boolean Logic and Organizing
- Multiple Workflows and Versioning
- Simulate Workflow
- Visualize Workflow

Fraud
Lens



Workflow

- Reject
- Refer
- Resubmit

Reject Conditions

If Any of the conditions are met then reject this transaction.



- 1904 SSN/ITIN was not provided at input
- 1906 DOB was not provided at input
- R704 Address is a correctional facility
- R901 SSN/ITIN cannot be resolved to the individual
- R907 SSN has been reported as deceased
- R909 Identity has been reported as deceased
- R911 SSN issued prior to DOB
- R913 SSN/ITIN is invalid
- R932 Address is a correctional facility
- R947 SSN/ITIN is not the primary SSN/ITIN for the resolved identity
- SCORE Fraud

Accept


Identity Proofing Accounts




Decision and Module data examples (not SERS data)

Transaction Information  









TRANSACTION ID	TRANSACTION DATE	CUSTOMER ID	ENVIRONMENT	ACCOUNT
a886b683-b7c8-4ccc-b902-480a4860b429	Apr 25, 2022 03:16:59 PM	-	Sandbox	School Employees Retirement System of Ohio

Queried Data 

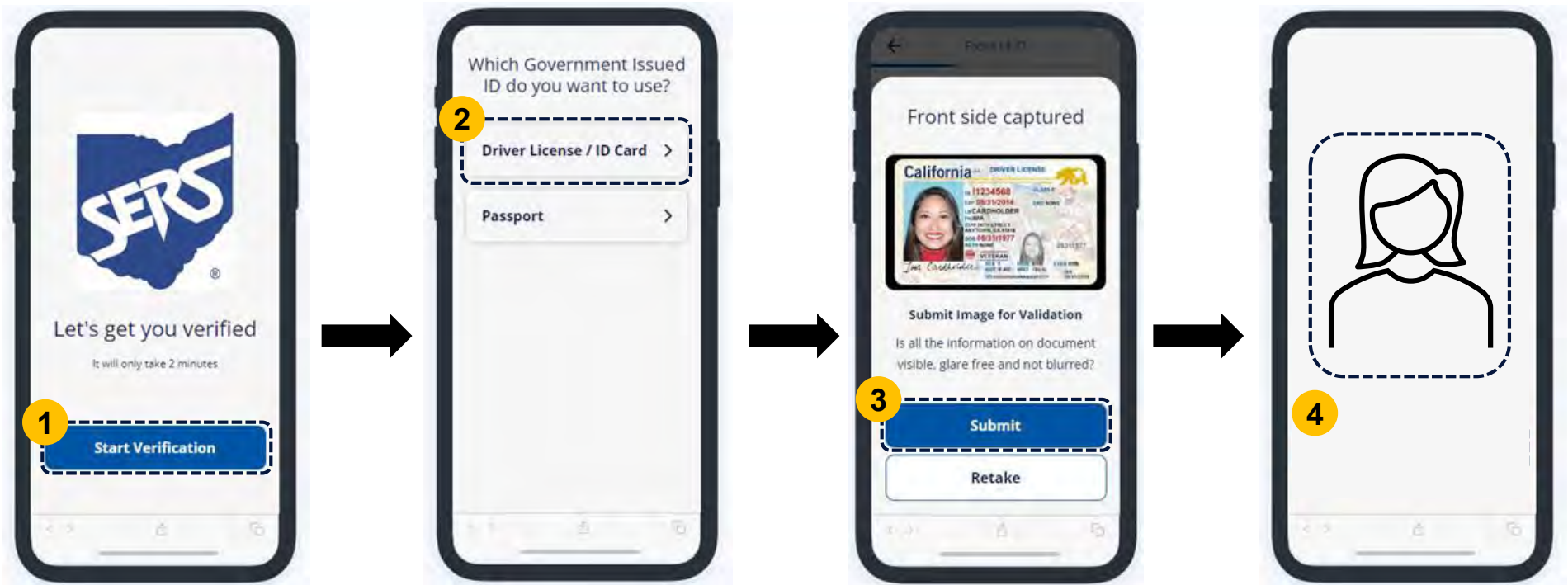
PERSONAL	Results
FIRST NAME: Joey	Fraud 1553, 1121, 1127
SUR NAME: Tester4	Email Risk MEDIUM 1520, 1353
ENTITY TYPE: .	Address Risk MEDIUM 1720, 1703, 1704
NATIONAL ID: ***-**-****	KYC INFO 1019
DATE OF BIRTH: **/**/****	Alert List NO MATCH
IP ADDRESS: **.*.*.*	Synthetic LOW 9228, 9223, 9229
CONTACT	
PHONE: .	
EMAIL: socured@ohsers.org	
ADDRESS: Street_S506817	
CITY: CITY_S506817	
STATE: OH	
ZIP: 00345	
COUNTRY: US	
OTHER	
USER ID: .	
DRIVER LICENSE: .	
DRIVER LICENSE STATE: .	

Decision ACCEPT 

LOGIC NAME : BASELINE V6 VERSION : 6

- SYNTHETIC :  ACCEPT
- FRAUD :  ACCEPT
- ADDRESS RISK :  ACCEPT
- ALERTLIST :  ACCEPT
- EMAIL RISK :  ACCEPT
- NAME EMAIL CORRELATION :  ACCEPT
- NAME ADDRESS CORRELATION :  ACCEPT
- KYC :  ACCEPT

Identity Proofing Accounts



Take Selfie – Compares selfie to ID photo

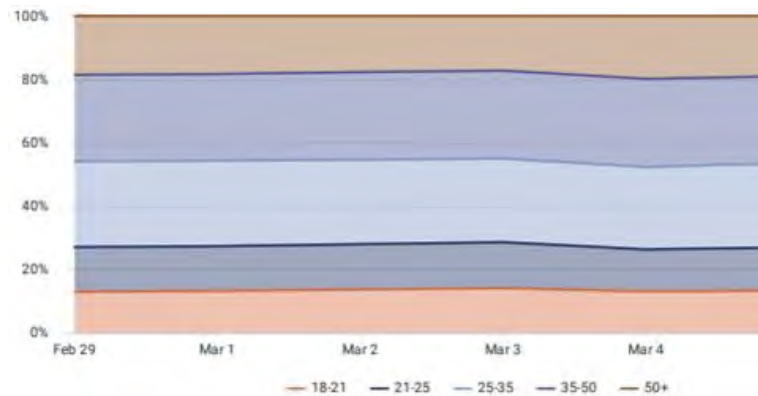
Step-up Verification with DocV (Takes Seconds, Not Minutes)

Identity Proofing Accounts



Examples of Fraud Analytics (not SERS data)

Age Demographic



Error Codes

Reason Code	Codes Description	Filing Rate
1 R208	SSN/ITIN is associated with multiple addresses	33.90%
2 R919	Unable to verify address	13.88%
3 R922	Unable to verify date of birth	12.51%
4 R610	IP address geolocation >100 miles from input address	11.77%
5 R660	Two or more addresses are marked as current the pho...	11.45%
6 R902	KYC record validation failed on Name	9.92%
7 R561	Email address <180 days old	9.46%
8 R606	Phone not actively used	8.98%
9 R705	Name associated with address does not match input ...	8.76%
10 R608	Name associated with phone does not match input na...	8.55%
11 R187	Address resolves to a High-Intensity Drug Trafficking A...	8.04%
12 R659	phone has been seen with more than two emails last e...	7.59%
13 R571	Email not actively used	6.95%
14 R607		6.44%

Email Domain Usage

Transaction Date	Email Domain	Percent of Count of Transaction ID
2024-02-29	gmail.com	60%
		15%
	yahoo.com	10%
	icloud.com	5%
	hotmail.com	2%
	outlook.com	2%
	aol.com	1%
	anshanuttauhid.com	0%
	live.com	0%

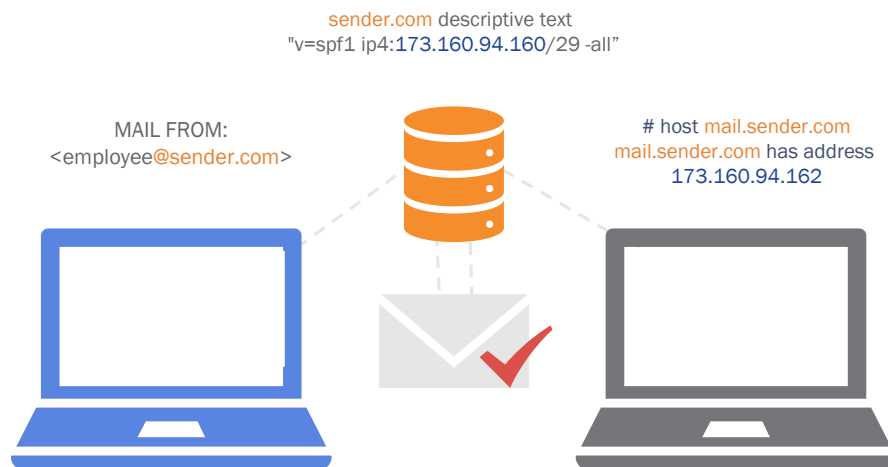
Country Telemetry

Transaction Date	Predictor	Count of Transaction ID
2024-02-29	US	191,827
	**	162,250
	PR	1,253
	CA	232
	MX	155
	JP	84
	UK	45
	IN	42
	DE	39
		27



Combating Email Threats

Combating Email Threats



Sender Policy Framework (SPF)

SPF allows organizations to declare (in DNS) what IP addresses can send on their behalf.

SPF Shortcomings

- Difficult to keep updated
- Messages are not always blocked
- Breaks when a message is forwarded

Combating Email Threats



Domain-based Message Authentication, Reporting & Conformance (DMARC)

DMARC ensures the 'From' address that **users see in their email client is trustworthy.**

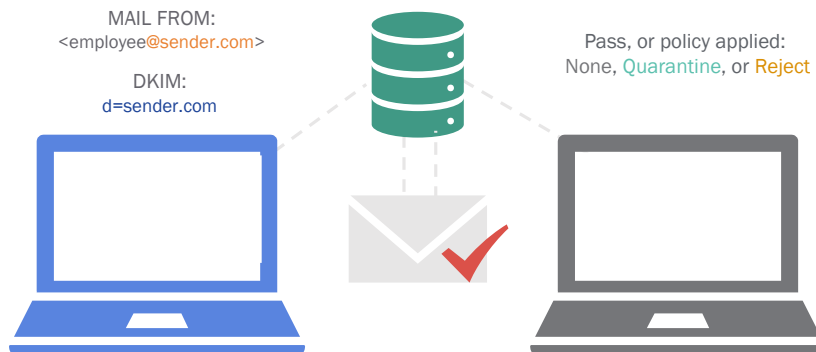
DMARC Benefits

- Allows for collection of DMARC reports to understand brand's email authentication ecosystem
- Instructs email providers on how to handle unauthenticated mail, removing any guesswork on how they should handle messages that fail DMARC authentication

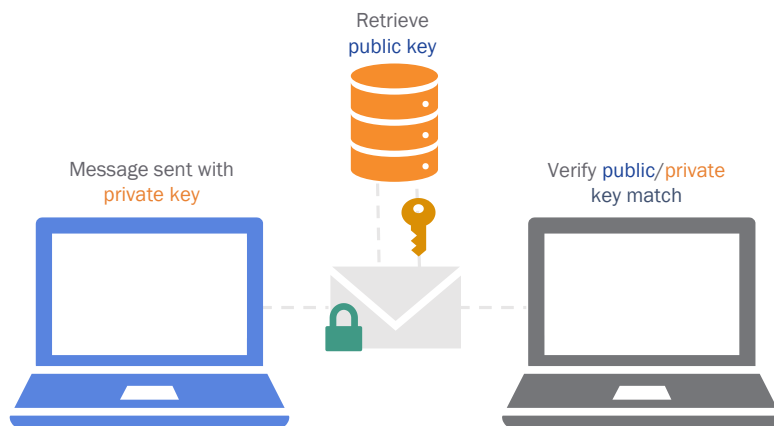
Header From: <employee@sender.com>

SPF: Pass and alignment check pass
Return-Path: <employee@sender.com>

DKIM: Pass and alignment check pass
d=sender.com



Combating Email Threats



DomainKeys Identified Mail (DKIM)

DKIM ensures that messages **aren't tampered with in transit**, utilizing cryptography.

DKIM Shortcomings

- Requires coordination between parties involved
- More complex
- DKIM not visible to non-technical end user

Combating Email Threats



Domain Risk Assessment for Inbound Email

Total 5,872 3rd-party domains.

By Risk Level. Click to See Details



By DMARC Policy



Gold Standard

```
v=spf1 include:%{ir}:%{v}:%{d}.spf.has.pphosted.com ~all
```

```
v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com
```

Example (SELS.US) - Needs Improvement

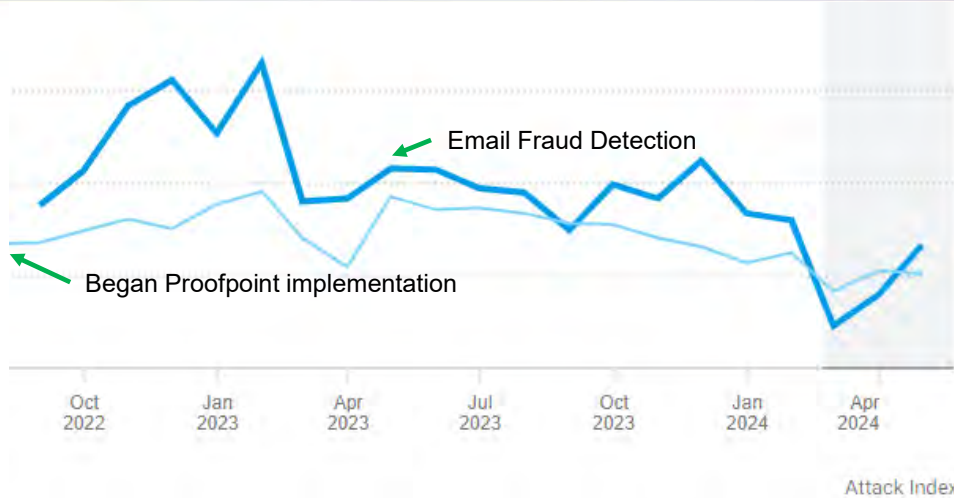
```
v=spf1 include:_spf.google.com include:mveca.org ~all
```

Emails Received by SERS

sels.us	lorainschools.org	paintvalleylocalschools.org	americantelemed.org	moe.gov.sa	cmich.edu
hyland.com	ct-e.ru	signupgenius.com	mkkcc.org	secureserver.net	moe.edu.eg
wsj.com	crinalerts.com	sscinc.com	tosoh.com	arizent.com	ubs.com
govdelivery.com	osu.edu	global-infra.com	govex.com	issmediasolutions.com	dowjones.com
ntrs.com	ihg.com	westernasset.com	nccourts.org	on24event.com	statnews.com
montgomerycountymd.gov	hondros.edu	mrsoftware.com	oaktreecapital.com	vrmailer3.com	issgovernance.com



Combating Email Threats



- Closed loopholes that allowed direct emailing
- Modified policies to prevent “spoofing” to employers and members
- Identified “shadow” functions sending emails on behalf of SERS
- Closed loopholes that allowed relaying of email

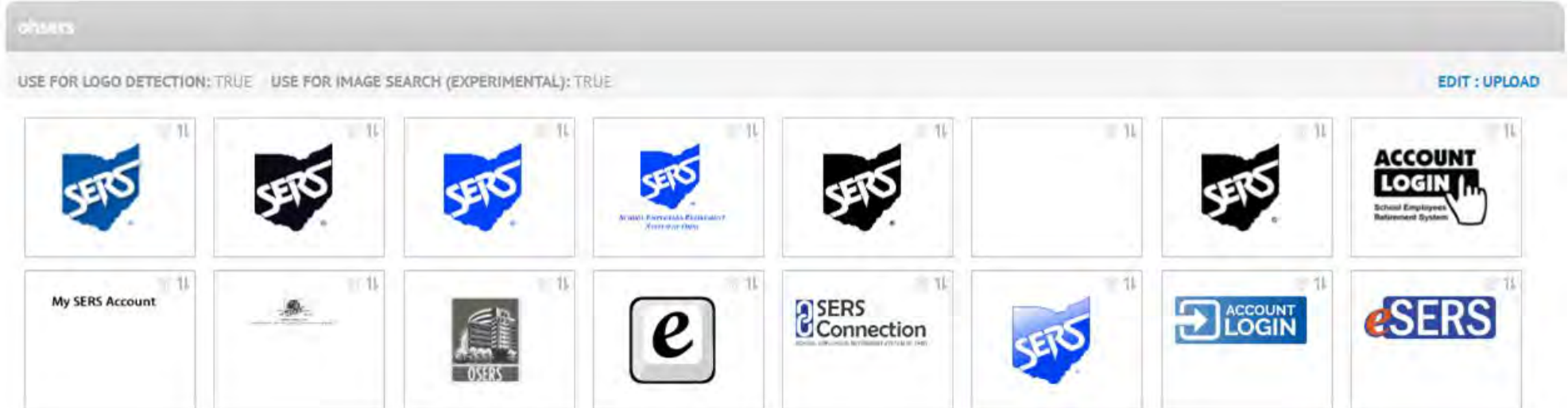
DOMAIN WATCHLIST
'oshers.org'
First Observed 8/14/2023
Zero Offenses

<p>3.3K messages from senders impersonating 'SERS' that have not been approved/permited that may put brand at risk.</p>		<p>1 registered domains that look like 'SERS' and may be used to impersonate our brand.</p>
<p>90-day period</p>		
	<p>75 messages from 'SERS' approved/permited senders that fail DMARC and may not get delivered.</p>	

Combating Email Threats



Protecting SERS' Brand and Detecting Spoofed Emails



Any Email Sent Through Proofpoint with Our Logo Will Be “Flagged/Alerted” If the Origin Isn’t On Our Approved List

Summary



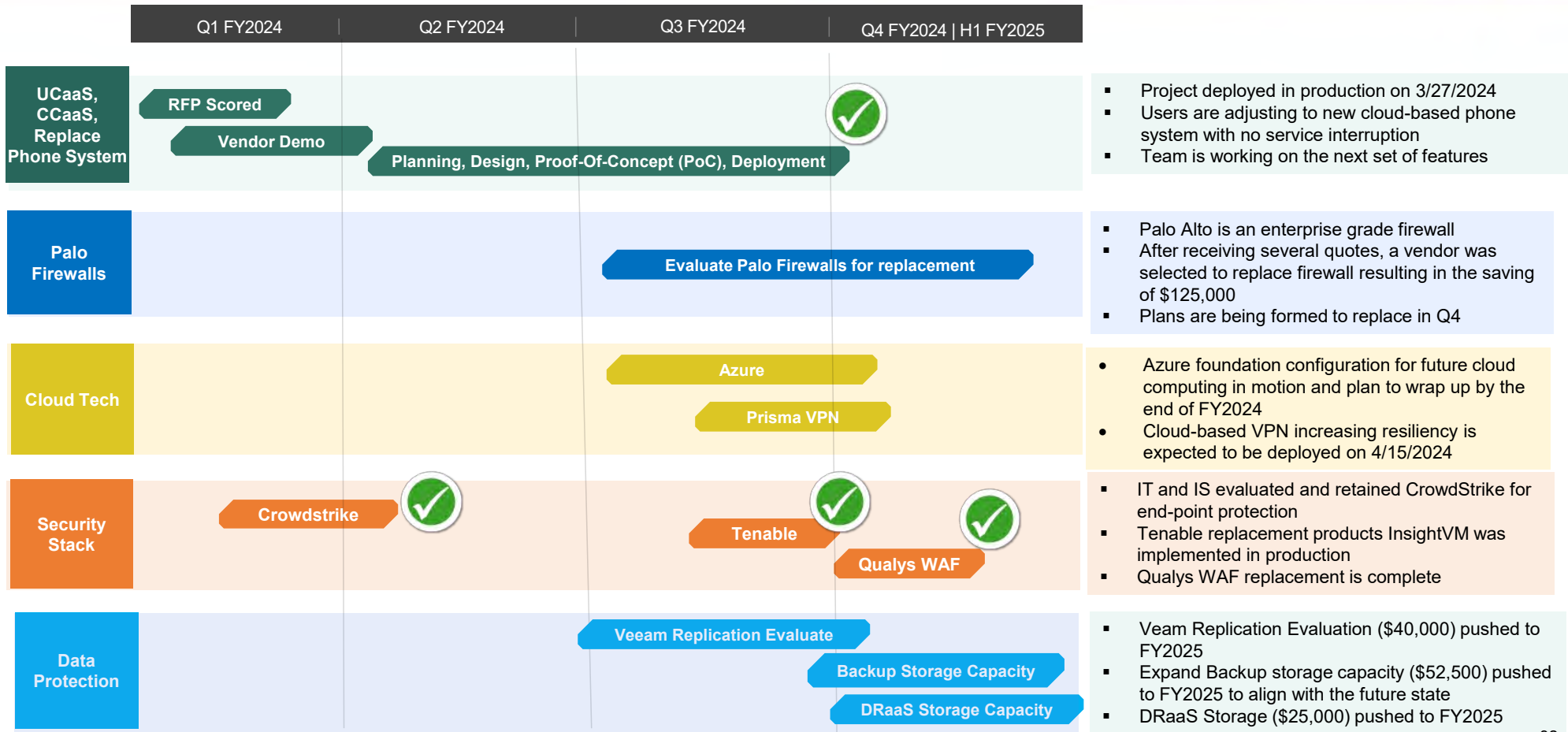
- Fraud continues to be real concern now and in the future.
- Awareness of fraud and prevention tools are important to SERS and our members.
- Artificial Intelligence will expand, presenting opportunities and challenges.
- Monitoring the dark web is an important part of our Fraud Risk and Cyber program.
- As SERS' electronic services expand, additional identity proofing measures are required.
- Email remains a valuable tool and improved monitoring capabilities continue to be upgraded.



INFORMATION TECHNOLOGY UPDATE

Technology Roadmap

Technology Roadmap – FY2024 Infrastructure Projects



Technology Roadmap – FY2024 SMART Projects

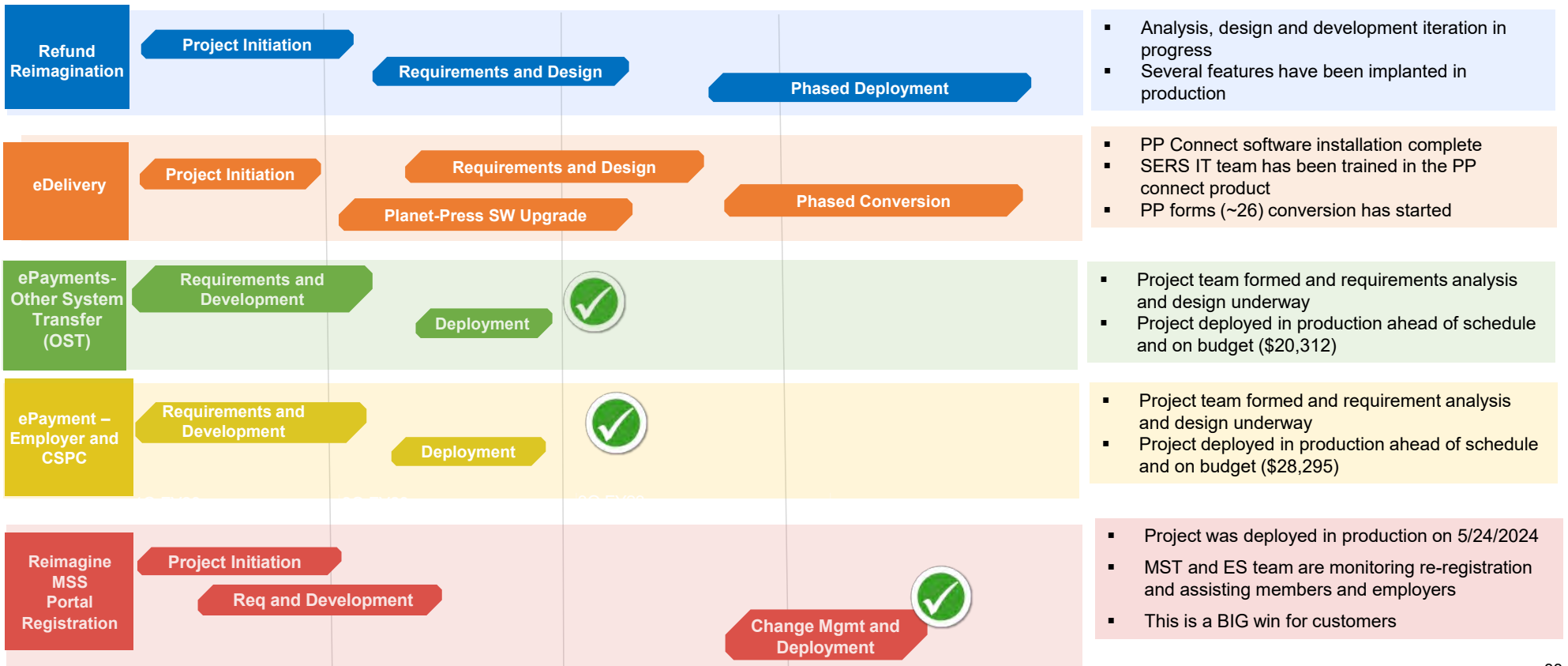


Q1 FY2024

Q2 FY2024

Q3 FY2024

Q4 FY2024



Portal Registration Reimagination



Confirm Your Identity

* Last Name:

* Social Security Number:

* Date of Birth:

* Zip Code:

Create a username for your Account Login. Your username should be at least six characters using numbers, letters, @, period, or underscore. No special characters (~ ! # \$, etc.)

* Username:

Password rules and tips: Must be at least 8 characters long.
Must contain an uppercase character.
Must contain a lowercase character.
Must contain a numeric character.
Cannot be the same as your username.
Cannot contain contact information.

* Password:

* Confirm Password:

Security Questions

Questions	Answer
At which of the following addresses have you resided 10+ years?	<input type="radio"/> 3375 Euclid St <input type="radio"/> 26100 Lorain Rd <input type="radio"/> 127 N 58th St <input type="radio"/> 9278 Liberty Station Rd
Which of these school districts have you worked for?	<input type="radio"/> New West City Schools <input type="radio"/> Cleveland Metropolitan School District <input type="radio"/> Southeast Ohio Council of Governments

Account Verification

Help us protect your account.

You will need a verification code to complete your account registration. How would you like to receive your code?

If you would like to update or add your contact information, call SERS at 1-800-878-5853.

n*****e@ohsers.org
 Call +161*****51
 Text +161*****51

Portal Registration Reimagination – Deployed



Strengthen security while improving user experience

- Approximately 11,000 calls per year for portal registration assistance (expecting ~60% call reduction in assistance with new enhancements)
- OKTA security software integrated
- Multi-factor authentication (MFA) - verification code for ongoing portal access
- Existing member and employer portal accounts deactivated
- Extensive change management and communication to onboard members and employers

Preliminary Metrics (5/24/24 - 6/07/24)

MST has successfully answered **340** MSS help calls. Theme of these calls: users trying to use old login information.

User Registration

- MSS
 - Active - 5,843
 - Registered - 175
- eSERS:
 - Active - 2,505
 - Registered - 1,459

Member Portal Journey: Online Account Refunds



- Current online capabilities
 - User can complete refund application and mail to SERS
- Near-term improvement (Q1 FY2025)
 - Refund application status on member portal (anticipate reduction in MST calls)
- End-to-end online refund processing with Socure (Target – H2 FY2025)
 - Refunds less than \$5,000 processed online by member
 - Identity verification and fraud prevention through Socure
 - Seamless user experience

Technology Roadmap Financial Tracking



Five Year Technology Roadmap Budget						
Description	Total 5-Year Plan	FY2023 Actual Spend	FY2024 Plan*	FY2024 Spend to Date	Total Roadmap Spend to Date	Remaining Roadmap Amount **
Telecommunications	\$ 250,000	\$ 175,848	\$ 206,491	\$ 128,508	\$ 304,356	\$ (132,339)
Security Stack	\$ 899,600	\$ -	\$ 432,200	\$ 70,977	\$ 70,977	\$ 467,400
Network Infrastructure Refresh	\$ 886,000	\$ 638,914	\$ 120,000	\$ 14,384	\$ 653,297	\$ 127,086
Hybrid Technology Replacement	\$ 419,000	\$ 121,297	\$ 10,000	\$ 2,203	\$ 123,499	\$ 287,703
Server Infrastructure	\$ 1,216,700	\$ -	\$ 288,100	\$ -	\$ -	\$ 928,600
Backup and Recovery	\$ 532,754	\$ 140,455	\$ 117,500	\$ -	\$ 140,455	\$ 274,799
SMART Portals	\$ 196,000	\$ -	\$ 196,000	\$ 26,250	\$ 26,250	\$ -
SMART Framework	\$ 760,000	\$ 175,000	\$ 510,000	\$ 175,000	\$ 350,000	\$ 75,000
SMART Enhancements	\$ 2,623,000	\$ 73,836	\$ 855,000	\$ 156,306	\$ 230,141	\$ 1,694,165
SMART Business Tools	\$ 500,000	\$ 96,400	\$ 250,000	\$ 215,682	\$ 312,082	\$ 153,600
SMART total	\$ 4,079,000	\$ 345,236	\$ 1,811,000	\$ 573,238	\$ 918,474	\$ 1,922,765
Infrastructure Total	\$ 4,204,054	\$ 1,076,514	\$ 1,174,291	\$ 216,071	\$ 1,292,584	\$ 3,987,983
Total Budget	\$ 8,283,054	\$ 1,421,749	\$ 2,985,291	\$ 789,309	\$ 2,211,058	\$ 3,876,014

* Two infrastructure projects have been realigned with category descriptions to better reflect their underlying expense.

The total FY2024 Plan did not change.

** Remaining Roadmap is equal the Total 5-Year Plan less FY2023 Actuals and less FY2024 Plan



RISK MANAGEMENT UPDATE

FY2024 Q4 Update – Risk Management



- School Cyber Incident Notification to SERS
 - Joint Committee On Agency Rule (JCARR) hearing is scheduled for June 24
 - Anticipate the final presentation to SERS Board at July 2024 meeting
- Dark Web Monitoring
- Information Security Metrics and Monitoring – April to June 2024

EXECUTIVE SESSION

_____ moved and _____ seconded the motion that the Technology Committee convene in Executive Session pursuant to R.C. 121.22(G)(6) to discuss a security matter.

Upon roll call, the vote was as follows:

<u>ROLL CALL:</u>	<u>YEA</u>	<u>NAY</u>	<u>ABSTAIN</u>
James Rossler	_____	_____	_____
Frank Weglarz	_____	_____	_____
Daniel Wilson	_____	_____	_____
Matthew King	_____	_____	_____

IN EXECUTIVE SESSION AT _____ A.M./P.M.

RETURN TO OPEN SESSION AT _____ A.M. / P.M.



QUESTIONS/ FUTURE TOPICS

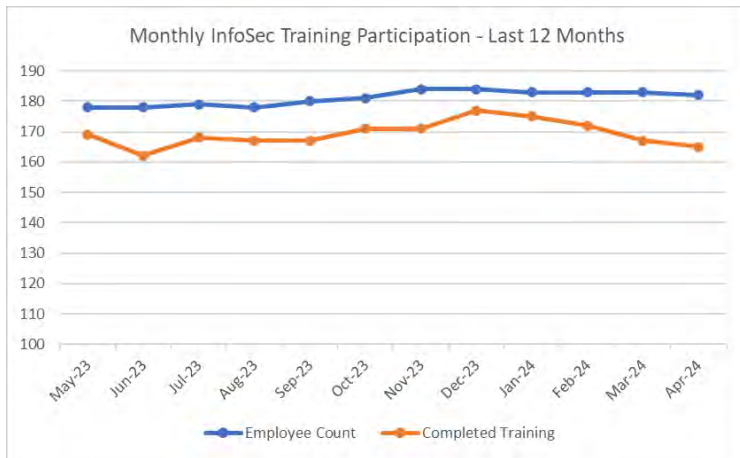
ADJOURNMENT(R)

_____ moved that the Technology Committee adjourn to meet on _____
for the next scheduled meeting.

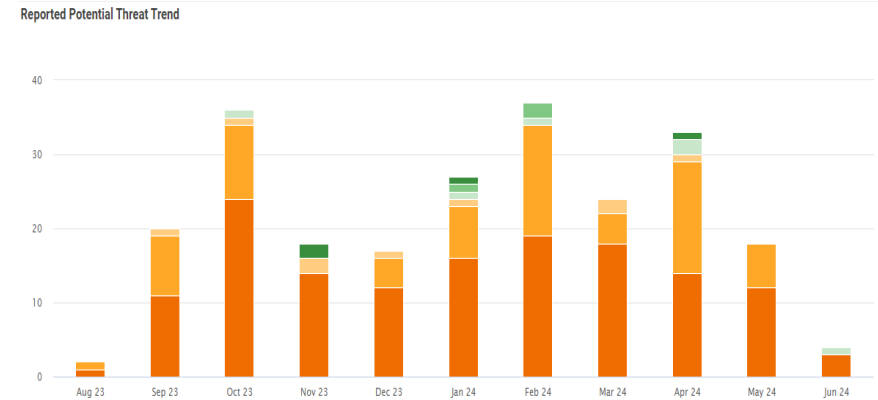
The meeting adjourned at _____ p.m.

Matthew King, Chair

Information Security – Key Metrics



Security Awareness Training > 90% Goal - MET



Phish Reporting & Response < 7-day goal – MET
(NOTE: Process Change/Improve Response to Hours - November)

Three Lines of Defense:

1. Proofpoint
2. Microsoft
3. Staff

Migration between vulnerability management tools is progressing. Expect charts at next meeting.

Metrics: Inbound Email and Blocked Messages



Reporting Period – 3/31/2024 – 6/11/2024

Inbound Email Protection Breakdown

