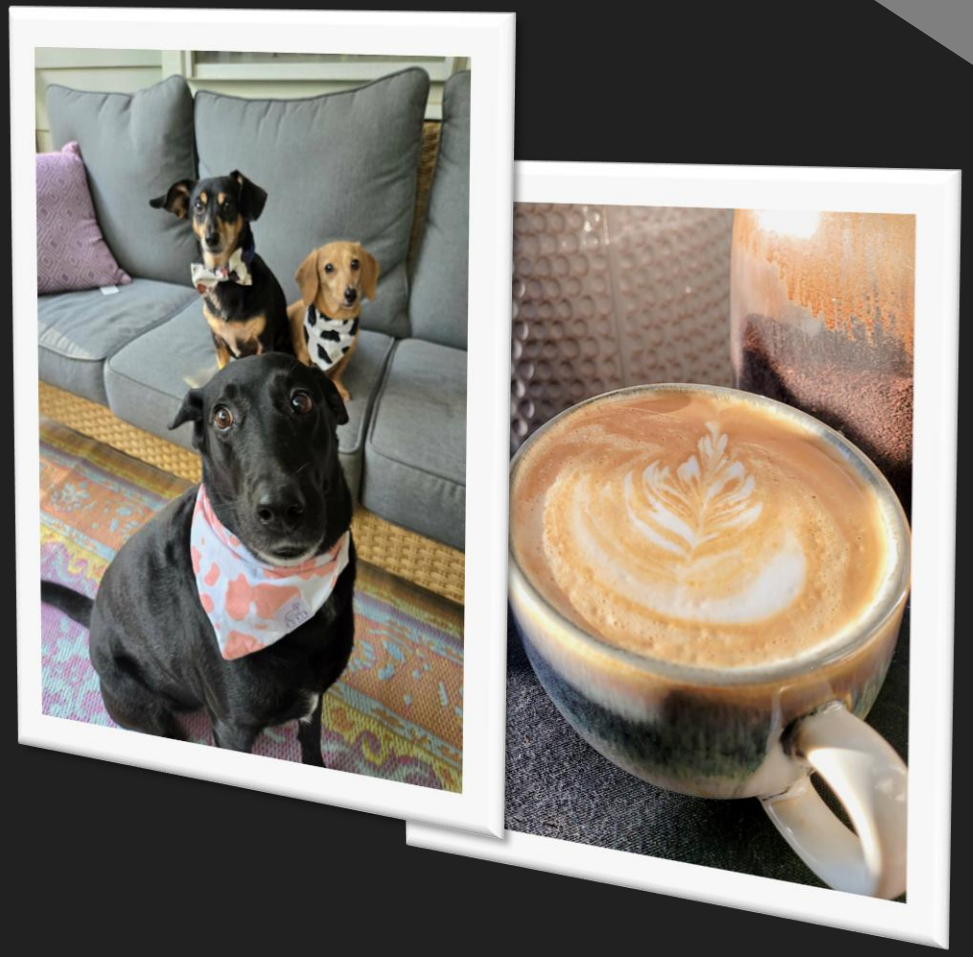
SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY (SC CIC)

Debon Grady
Cyber Threat Intelligence Analyst

About Me

1. GRADUATE OF WESTERN GOVERNORS UNIVERSITY
2. MINECRAFT SERVER ADMINISTRATOR
3. SECONDARY TREAT DISPENSER
4. AMATEUR LATTE ARTIST



Agenda

1. SC CIC Services Overview
2. Financial Fraud & Spear Phishing 101
3. Cyber Terrorism in South Carolina
4. Real Impacts of Ransomware: The Fallout of Fairlife

What We Do

1. Provide **security services & disseminate cyber threat intelligence** to South Carolina's **Critical Infrastructure Sectors** at **no cost to the organization**

2. Facilitate the **Cyber Liaison Officer (CLO)** Program

3. Lead the **SC CIC Task Force**, comprised of Federal and State Partners

4. improve the **overall cyber posture** of South Carolina

SC CIC BY SECTOR



SC CIC Task Force



SC Law Enforcement Division
Oversees the SC CIC Program

SC Department of Administration
Division of Information Security

SC National Guard
125th Cyber Protection Battalion

US Department of Homeland Security
Cybersecurity & Infrastructure Security Agency

US Secret Service
Cyber Fraud Task Force

US Department of Homeland Security
Office of Intelligence and Analysis

SC Emergency Management Division
Cyber Incident Consequence Management

Federal Bureau of Investigations
Cyber Squad

SC Election Commission
Election and Voter Information Security

SC CIC Services

PHISHING & CYBERSECURITY TRAINING

THREAT INTELLIGENCE

READINESS EXERCISES

VULNERABILITY SCANNING

ACTIVE DIRECTORY SECURITY ASSESSMENT

MICROSOFT 365 SECURITY ASSESSMENT



Cyber Liaison Officer (CLO) Program

The **CLO** program has been critical in:

- **Facilitating information sharing** between SC CIC and private and public critical infrastructure organizations.
- Giving **SC CIC Task Force partners** the opportunity to leverage the CLO program to **share intelligence bulletins** and **establish relationships**.
- Creating **networking and training opportunities** for cybersecurity professionals across the state through **conferences**, **workshops**, and **presentations**.



External Partners

The goal of an External Partner is to :

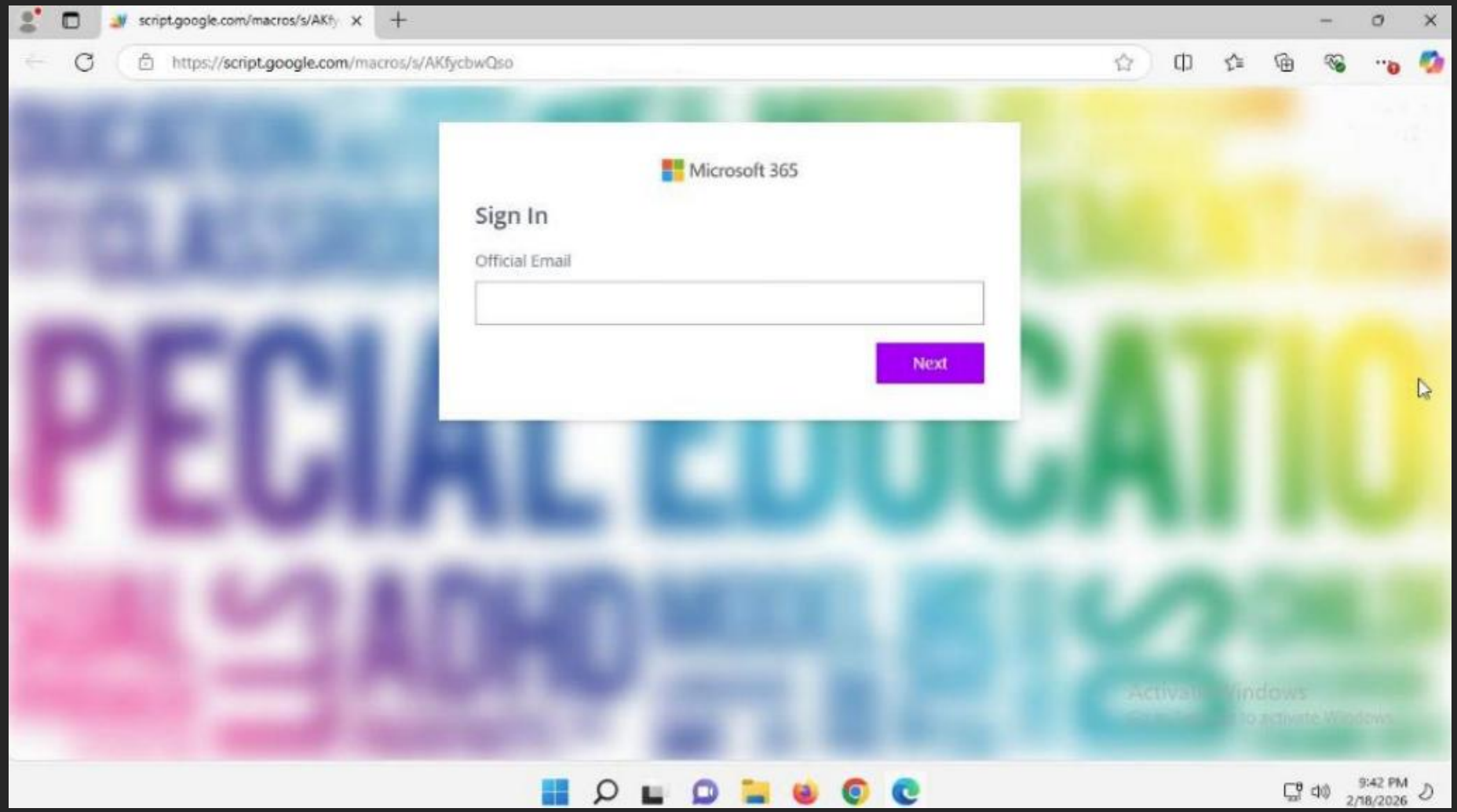
- Assist in disseminating SC CIC threat intelligence bulletins to critical infrastructure organizations in South Carolina.
- Provide **feedback** surrounding **cyber-related needs and gaps** in support for their respective sector.
- **Strengthen relationships** between **SC CIC, state associations, and federal agencies.**



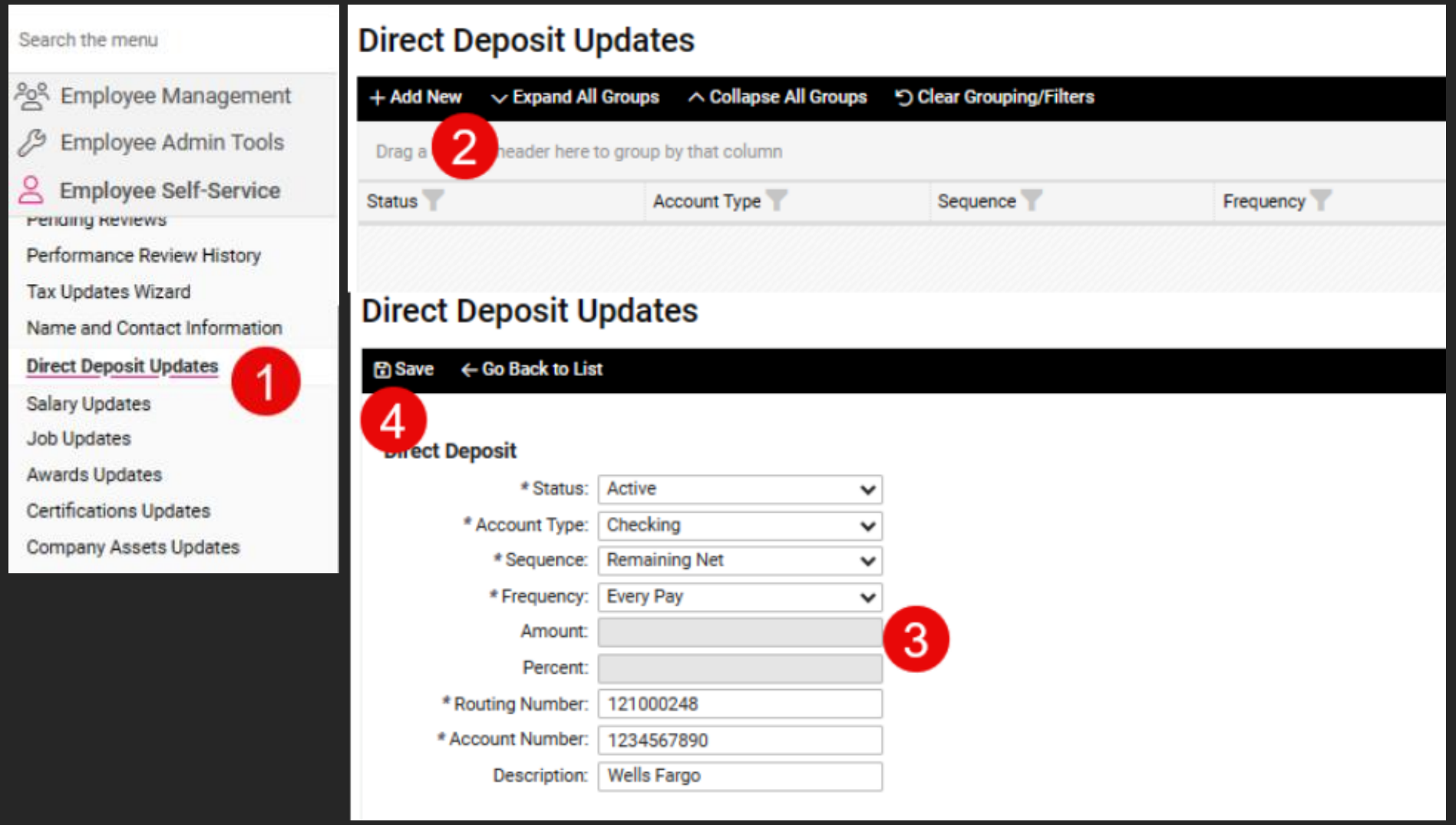
PAYMENT

FRAUD

User Compromise



User Compromise



User Compromise



GO2 BANK

How to set up direct deposit

Complete and submit the form below to your employer or government benefits provider to set up direct deposit to your GO2bank™ account. Please note the name and Social Security number on file with your employer or benefits provider must match your GO2bank account to prevent fraud restrictions on the account.

Account Information

Name
Robyn

Bank name
Green Dot Bank

Account number
15216862424282

Routing number
124303162

Account type
Checking

Amount

(X) Deposit my entire paycheck.

( ) Deposit _____% of my paycheck.

( ) Deposit $_____ of my paycheck.

It can take up to 2 pay periods for your pay to be direct deposited to your GO2bank account.

Voided check

GO2bank
Robyn Piers

123

DATE _____

PAY TO THE ORDER OF _____ $ _____

_____ DOLLARS

MEMO _____

⑆124303162 ⑆15216862424282 ⑈ 123

The image of this voided check may be provided to your employer or other payor to set up direct deposit to your GO2bank account. The voided check cannot be used for any other purpose.

User Spoofing

From: Brian <godwo5367@gmail.com>
Sent: Tuesday, February 3, 2026 9:05 AM
To: @sled.sc.gov>
Subject: Re: payroll update

You don't often get email from godwo5367@gmail.com. Learn why this is important

CAUTION: This email originated from outside of SLED. Do not click links or open attachments unless you recogniz

Good morning [redacted]

I hope you're doing well today. I wanted to ask if you have had a chance to update my new direct deposit information that was submitted on the authorization form.

Thank you for your help!

Best regards,
Brian

User Spoofing



GO2 BANK

How to set up direct deposit

Complete and submit the form below to your employer or government benefits provider to set up direct deposit to your GO2bank™ account. Please note the name and Social Security number on file with your employer or benefits provider must match your GO2bank account to prevent fraud restrictions on the account.

Account Information

Name
Brian

Bank name
Green Dot Bank

Account number
151061877O0107

Routing number
124303162

Account type
Checking

Amount

- ☑ Deposit my entire paycheck.
- ○ Deposit _____% of my paycheck.
- ○ Deposit $_____ of my paycheck.

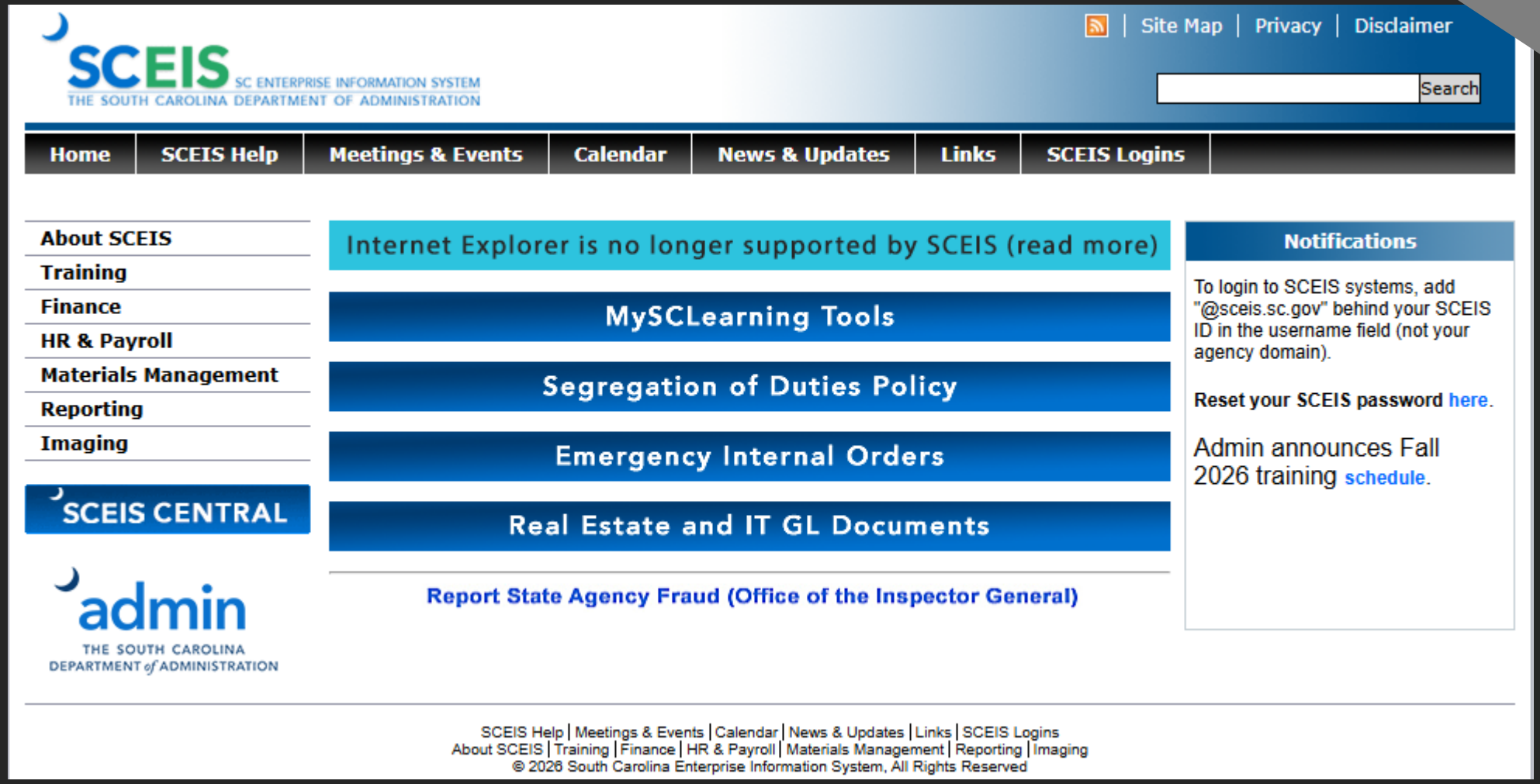
It can take up to 2 pay periods for your pay to be direct deposited to your GO2bank account.

Voided check

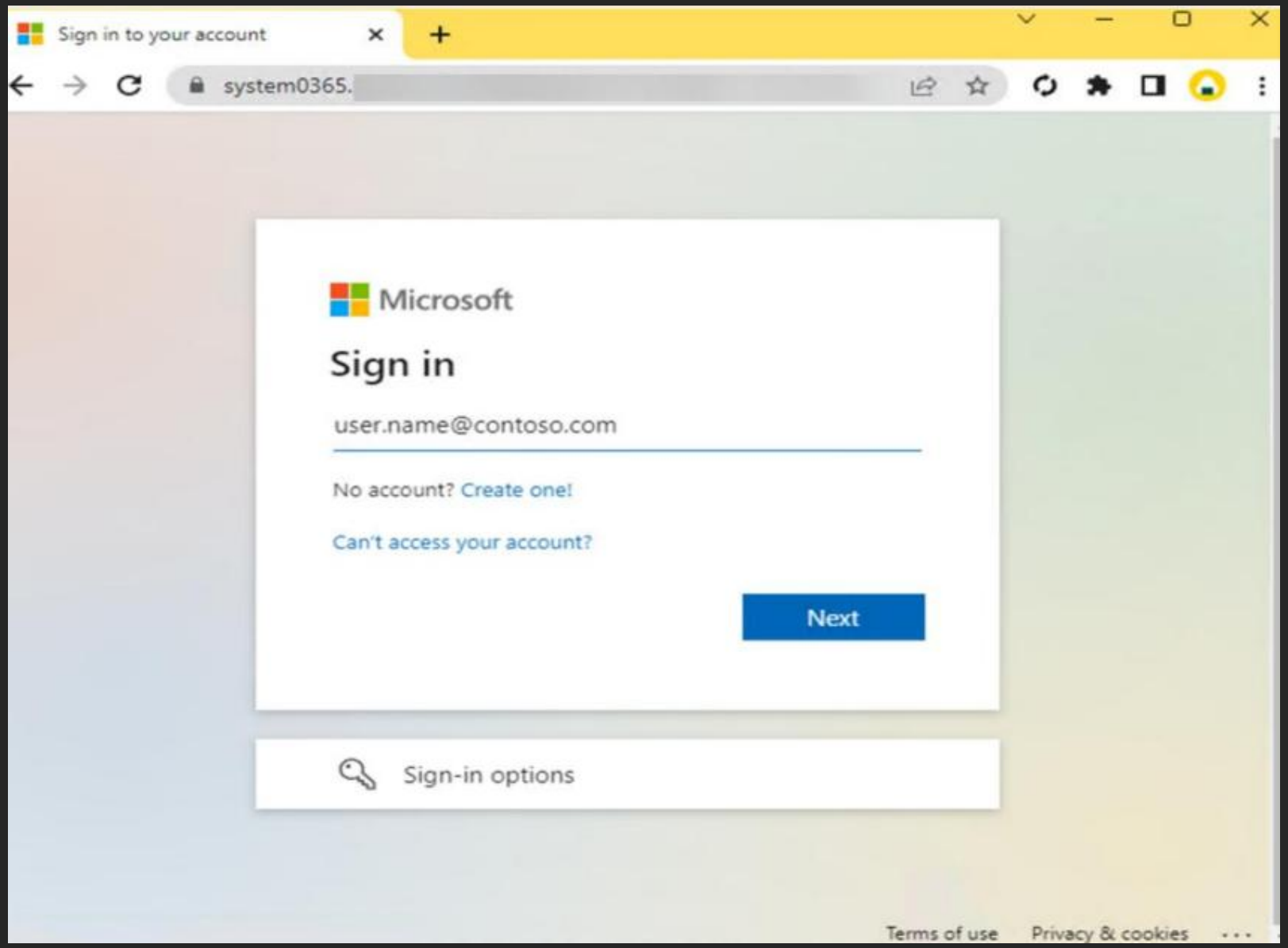
GO2bank
123
Brian Truex
304 SE NYE AVE
Pendleton , OR 97801
DATE _____
PAY TO THE ORDER OF _____ $ _____
_____ DOLLARS
MEMO _____
⑆ 124303162 ⑆ 151061877O0107 ⑈ 123

The image of this voided check may be provided to your employer or other payor to set up direct deposit to your GO2bank account. The voided check cannot be used for any other purpose.

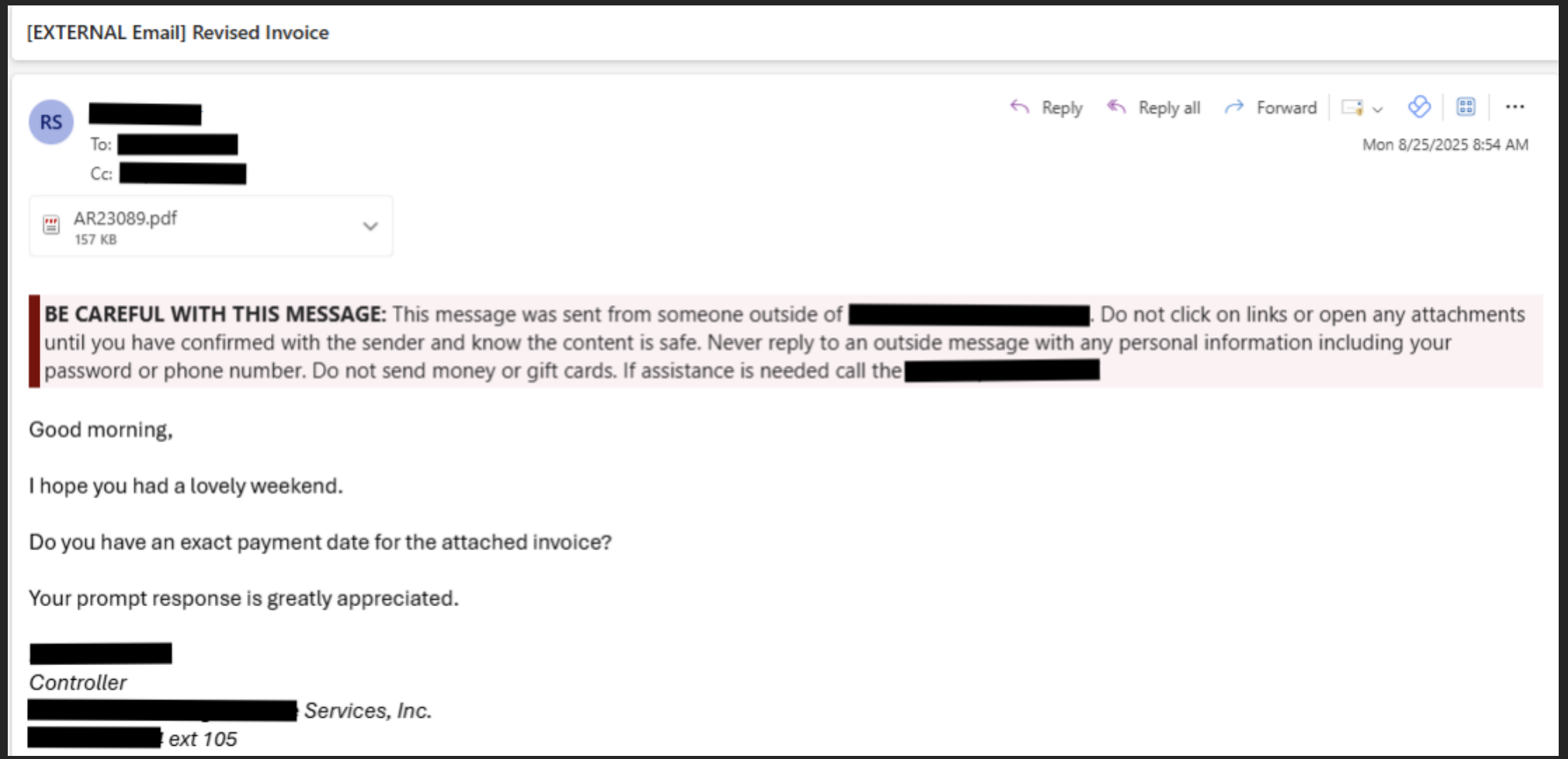
User Spoofing



Vendor Compromise



Vendor Compromise



[EXTERNAL Email] Revised Invoice

RS [redacted]

To: [redacted]

Cc: [redacted]

Reply Reply all Forward

Mon 8/25/2025 8:54 AM

AR23089.pdf
157 KB

BE CAREFUL WITH THIS MESSAGE: This message was sent from someone outside of [redacted]. Do not click on links or open any attachments until you have confirmed with the sender and know the content is safe. Never reply to an outside message with any personal information including your password or phone number. Do not send money or gift cards. If assistance is needed call the [redacted]

Good morning,

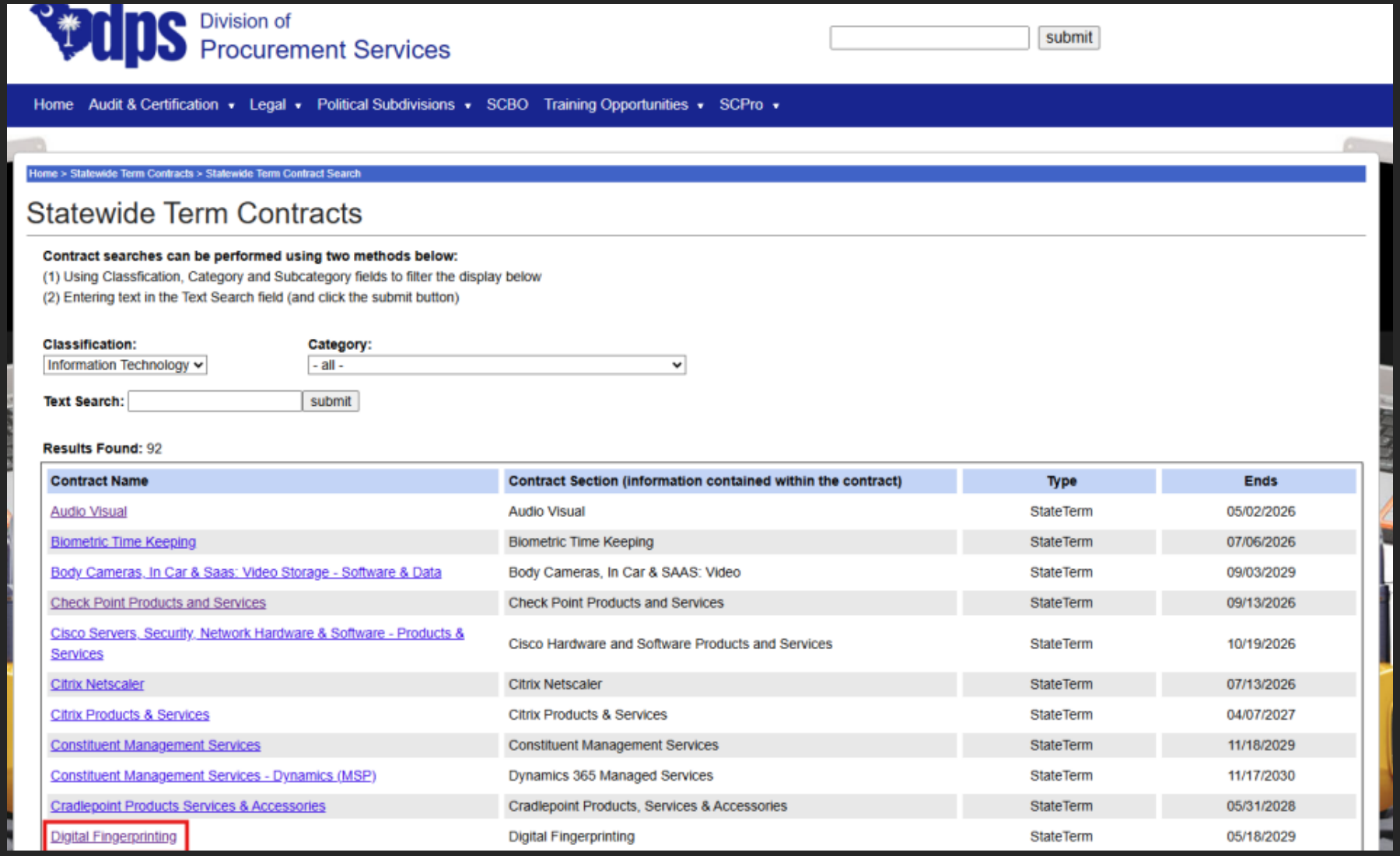
I hope you had a lovely weekend.

Do you have an exact payment date for the attached invoice?

Your prompt response is greatly appreciated.

[redacted]
Controller
[redacted] *Services, Inc.*
[redacted] *ext 105*

Vendor Spoofing



dps Division of Procurement Services

submit

Home | Audit & Certification | Legal | Political Subdivisions | SCBO | Training Opportunities | SCPro

Home > Statewide Term Contracts > Statewide Term Contract Search

Statewide Term Contracts

Contract searches can be performed using two methods below:
(1) Using Classfication, Category and Subcategory fields to filter the display below
(2) Entering text in the Text Search field (and click the submit button)

Classification: Information Technology

Category: - all -

Text Search: submit

Results Found: 92

Contract Name	Contract Section (information contained within the contract)	Type	Ends
Audio Visual	Audio Visual	StateTerm	05/02/2026
Biometric Time Keeping	Biometric Time Keeping	StateTerm	07/06/2026
Body Cameras, In Car & Saas: Video Storage - Software & Data	Body Cameras, In Car & SAAS: Video	StateTerm	09/03/2029
Check Point Products and Services	Check Point Products and Services	StateTerm	09/13/2026
Cisco Servers, Security, Network Hardware & Software - Products & Services	Cisco Hardware and Software Products and Services	StateTerm	10/19/2026
Citrix Netscaler	Citrix Netscaler	StateTerm	07/13/2026
Citrix Products & Services	Citrix Products & Services	StateTerm	04/07/2027
Constituent Management Services	Constituent Management Services	StateTerm	11/18/2029
Constituent Management Services - Dynamics (MSP)	Dynamics 365 Managed Services	StateTerm	11/17/2030
Cradlepoint Products Services & Accessories	Cradlepoint Products, Services & Accessories	StateTerm	05/31/2028
Digital Fingerprinting	Digital Fingerprinting	StateTerm	05/18/2029

Vendor Spoofing

Description:

Lot A of this contract is for electronic fingerprinting services pursuant to state and federal laws, which require a state and national fingerprint-based fingerprint check. The fingerprinting image and demographic data must meet the FBI and South Carolina Law Enforcement Division (SLED) certification requirements. Qualified agencies, organizations, or individuals that require fingerprinting services contact the Contractor to arrange an appointed time and place for the fingerprinting to be performed.

Lot B and C of this contract are for SLED use only. Lot B is for an automated application and credentialing system for concealed weapons permits. Lot C is for an automated application and credentialing system for security guard licensing, private investigator licensing, and SC State Constable Commissions.

Partner Locations

Third party partner locations may be established by the Contractor to enhance service options, to ensure coverage requirements are met, and to increase location availability throughout all regions in the state. The locations must adhere to the most currently published FBI CJIS Security Policy and be reviewed by SLED for final approval. All personnel/agents must follow the same performance and training requirements as noted throughout the contract.

Digital Fingerprinting

Start Date: 05/19/2022 | **End Date:** 05/18/2029

Solicitation#: 5400021691

To schedule an appointment for fingerprinting services visit https://sc.ibtfingerprint.com. Applicants who have inquiries or would like assistance with scheduling can call (866) 254-2366.

Vendor: Idemia Identity and Security USA LLC

Contract#: 4400027894

Vendor#: 7000259392

Address: 296 Concord Road Suite 300 Billerica MA 01821

Phone#: (615) 372-8092

Contact: Jay Truitt

Phone#: (629) 235-2482

Email: jay.truitt@ps-idemia.com

Vendor Spoofing

Send

From jay-truitt@psimedia.com

To procurement@sled.sc.gov

Cc

Bcc

Subject Idemia Identity SLED Contract#: 4400027894 Payment Change

Idemia Identity and Security USA LLC 2026 Bank Details.pdf
210 KB

Good afternoon,

I am reaching out in regard to Contract#: 4400027894 we have in place with SLED. We are going to be changing our bank account details at renewal.

Attached are our new bank account details.

Thanks,

Jay Truitt
(615) 372-8092
Idemia Identity and Security USA LLC
296 Concord Road Suite 300 Billerica MA 01821

IDEMIA

Vendor Spoofing

Our top 20 domain names

First impressions count—make your mark with mail.com

Here at mail.com, we think that different email domains are a great way to bring a little personality to your email address or to give it a professional touch. We offer more than 100 domain names, but these are the undeniable favorites:

accountant.com	consultant.com	europe.com	musician.org
africamail.com	contractor.net	execs.com	myself.com
artlover.com	dr.com	hackermail.com	post.com
asia.com	email.com	iname.com	techie.com
cheerful.com	engineer.com	mail.com	usa.com

HTTPS://WWW.MAIL.COM/MAIL/DOMAINS/

How to Reduce Fraud Risk

Process & Policy Controls

- Require verification for all payment or vendor banking changes
- Verify requests using a known phone number on file, not information provided in the email
- Enforce out-of-band confirmation for messages involving:
  - Urgency or secrecy
  - Financial or payroll changes
  - Links or attachments

How to Reduce Fraud Risk

Access & Oversight

- Apply role-based access control:
  - Limit who can approve invoices, process payments, or modify vendor details
  - Fewer authorized users = fewer attack paths
  - Ensure users receive automated alerts if their direct deposit information is updated

How to Report Financial Fraud

- Report to SC CIC
- Report to Federal Trade Commission (FTC)
  - https://reportfraud.ftc.gov
- Report to FBI Internet Crime Complaint Center (IC3)
  - https://www.ic3.gov
- Time is of the essence

CYBER TERRORISM IN SOUTH CAROLINA

What is Operational Technology?

Physical world

↓

Input data through sensors

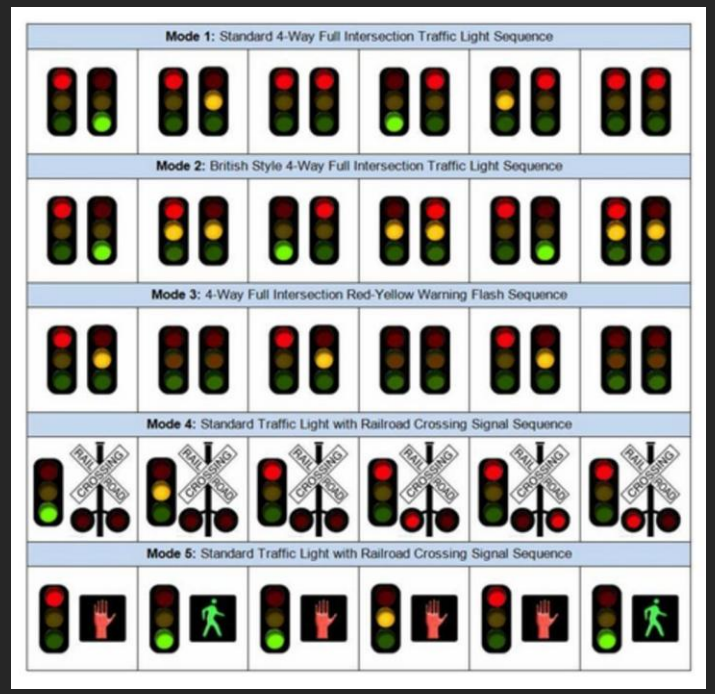
↓

Processed through logic

↓

Physical world





Industrial Control Systems = ICS



POORLY CONFIGURED PLCS

- On **Easter Sunday 2026**, several water/wastewater service providers noticed anomalies in their Operational Technology (OT) systems

- After investigation, it was determined that all effected systems were linked to a mutual 3rd party **Managed Service Provider (MSP)**

- **SC CIC** made an on-site visit to collect logs and perform **Root Cause Analysis (RCA)**
  - More than **160 PLCs** exposed directly to the internet
  - Many forensic artifacts were **destroyed in recovery efforts**
  - Other **Indicators of Compromise (IoCs)** were lost due to limited logging capabilities on Programmable Logic Controllers (PLCs)

POORLY CONFIGURED PLCS

- These Tactics, Techniques and Procedures (TTPs) would later be observed in several other high-profile water intrusions across the country
- July 2026 – Threat actors begin enumerating for open Programmable Logic Controllers (PLCs) exposed to the internet and locking operators out



CBS Evening News

At least 12 states report cyberattacks on water systems possibly linked to Iran-backed hackers, sources say

By Nicole Sganga

Updated on: August 6, 2026 / 10:02 AM EDT / CBS News

POORLY CONFIGURED PLCS

- Two South Carolina agricultural facilities experienced cyber attacks related to exposed OT systems in mid-August
- Similar scenario: both organizations managed by a mutual MSP over the OT systems, both configured similarly
- Threat actor modified refrigeration systems in such a way that would cause catastrophic harm to the facility

REAL WORLD IMPACT



THE TAKEAWAYS

- This was **intentional**
- The threat actor either knew exactly what they were doing, or used AI to give them insight to the process
- Check your **OT exposure**
  - We will do this for you if you're enrolled in Threat Intelligence!

FALLOUT OF

FAIRLIFE

Fallout of Fairlife

- In early July 2026, Fairlife experienced a network intrusion that resulted in ransomware

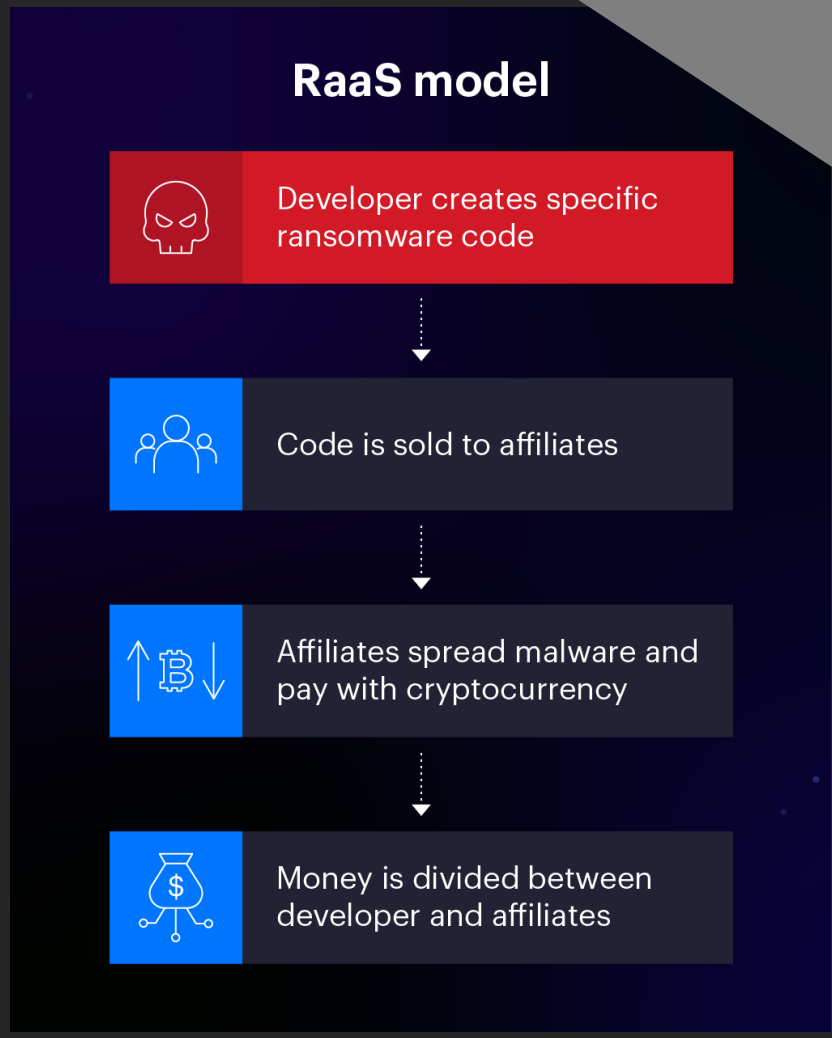
- Stopped production at all four U.S. Fairlife plants
  - Production shutdown for at least 11 days
  - Per Coca-Cola's SEC filing, product quality and safety were not impacted.

- Attack claimed by Anubis ransomware group
  - Ransomware-as-a-Service (RaaS)
  - Exfiltrated 1 Terabyte of data
  - Ransom was not paid, data was posted



What is RaaS?

- In the Ransomware-as-a-Service (Raas) model:
  - Affiliates keep 80% of ransom proceeds
  - Anubis operators keep 20%
- Anubis often handles the data-extortion "program"
- Ransomware groups are functionally no different than enterprise IT companies



How did they get in?

- A security flaw in Citrix NetScaler called CitrixBleed 2
  - (CVE-2025-5777) - Patches available June 17, 2025
  - NetScaler: network appliance many companies use for secure remote access

- Allowed Anubis to steal session tokens
  - Digital hall pass
  - Same technology used in social media & email

- Proves an improper response from Coca-Cola security
  - The patch only closed the hole for new thefts
  - Any tokens stolen prior to patching were valid

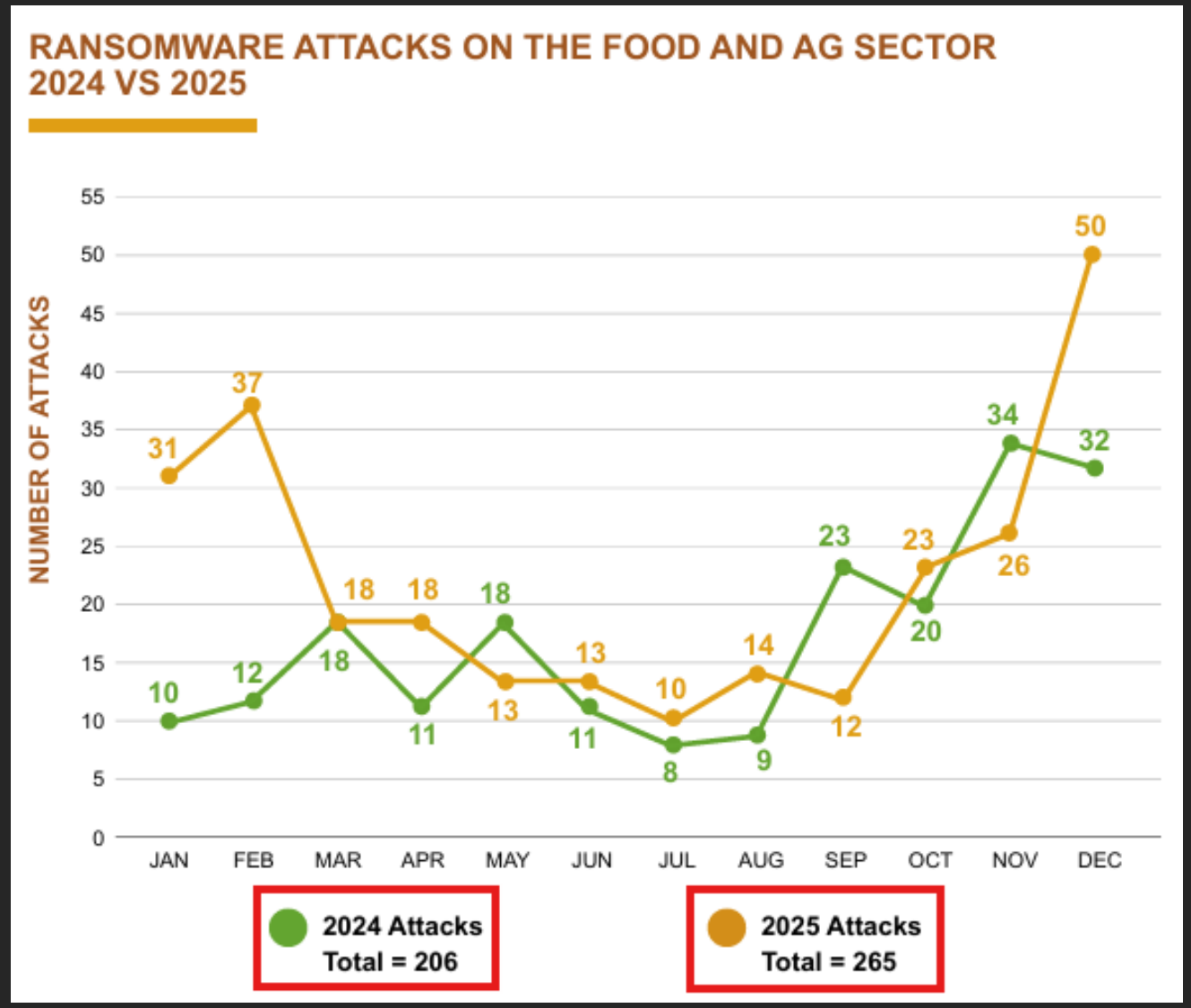


Food & Ag-ISAC



- Information Sharing and Analysis Center (ISAC)
- Sector-specific groups designed to share information regarding:
  - Current threat landscape and trends
  - Incident Response and Rapid Response communications
- Even if you choose not to join SC CIC (🥺), PLEASE consider getting in the loop with Food & Ag-ISAC

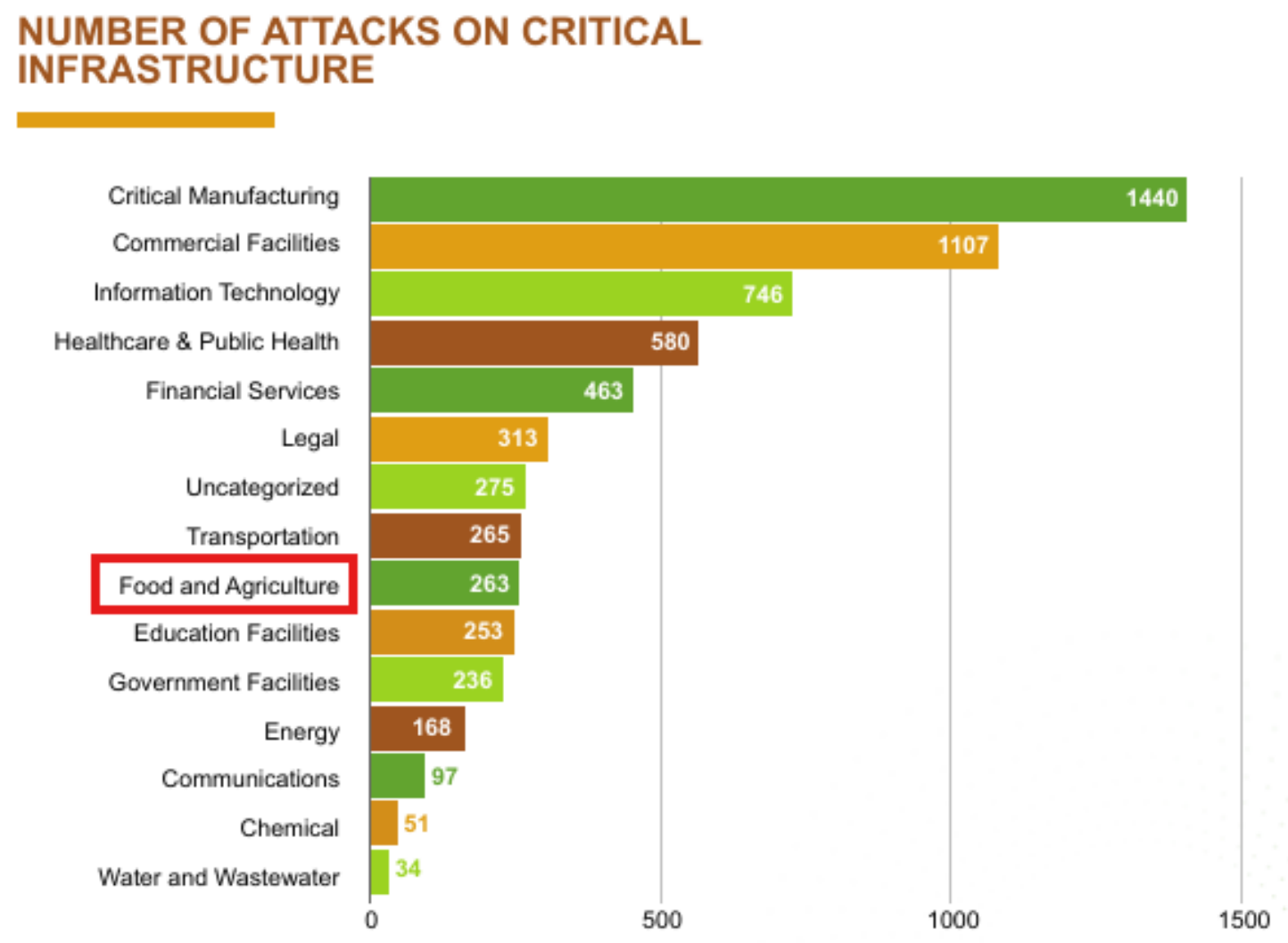
Farm-to-Table Ransomware Realities



The sector has been hit with over 200 attacks as of mid-July 2026

Food Ag-ISAC

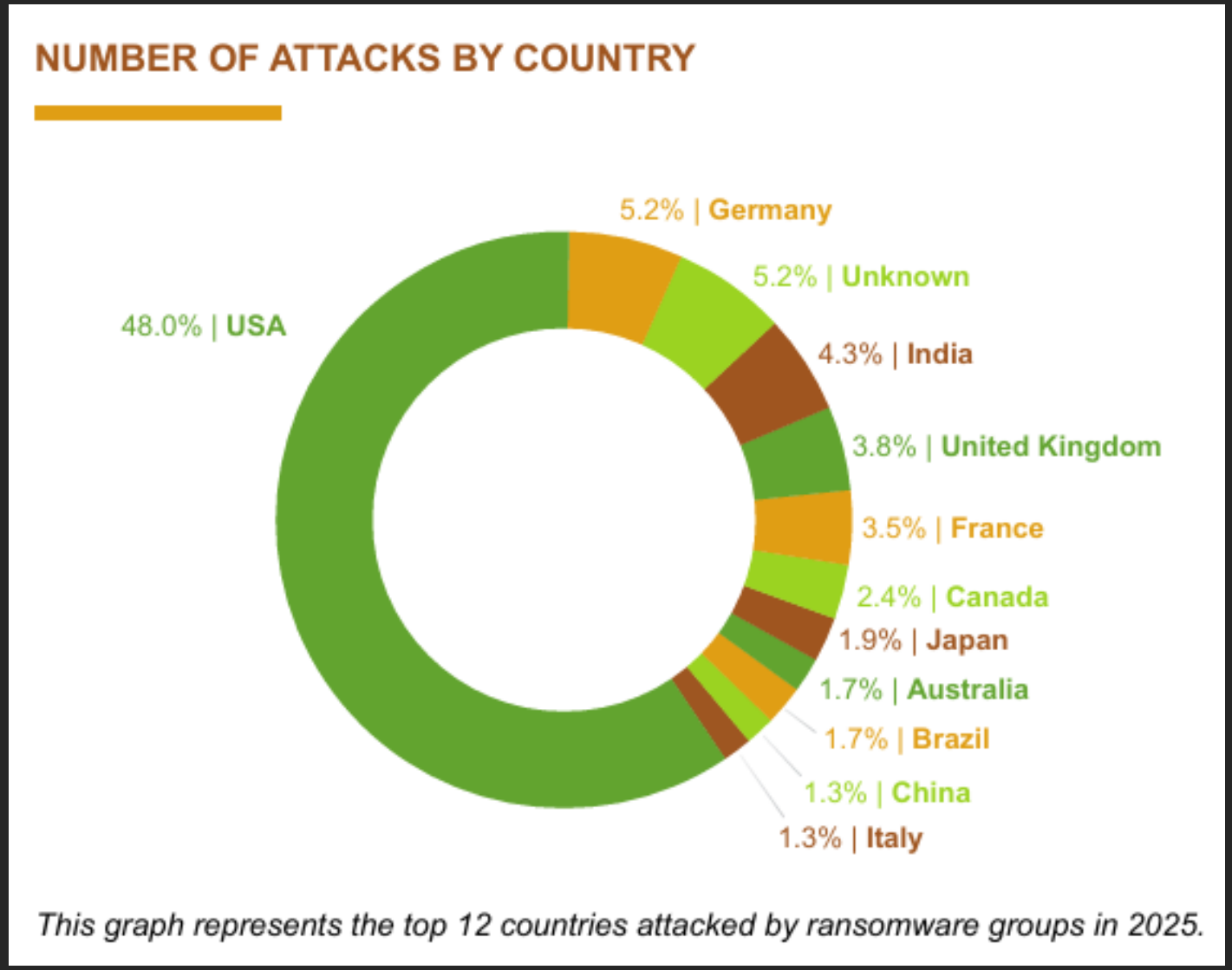
Farm-to-Table Ransomware Realities



Food and Agriculture accounts for ~5% of all ransomware attacks recorded in 2025

Food Ag-ISAC

Farm-to-Table Ransomware Realities



The Real Impact of Ransomware

- The following images were pulled from the Anubis Data Leak Site (DLS)
- Any redactions from this point forward were done by me
- I did not download the entire dataset
  - This presentation contains exclusively “sample” data that Anubis posted

Proprietary Industrial Processes



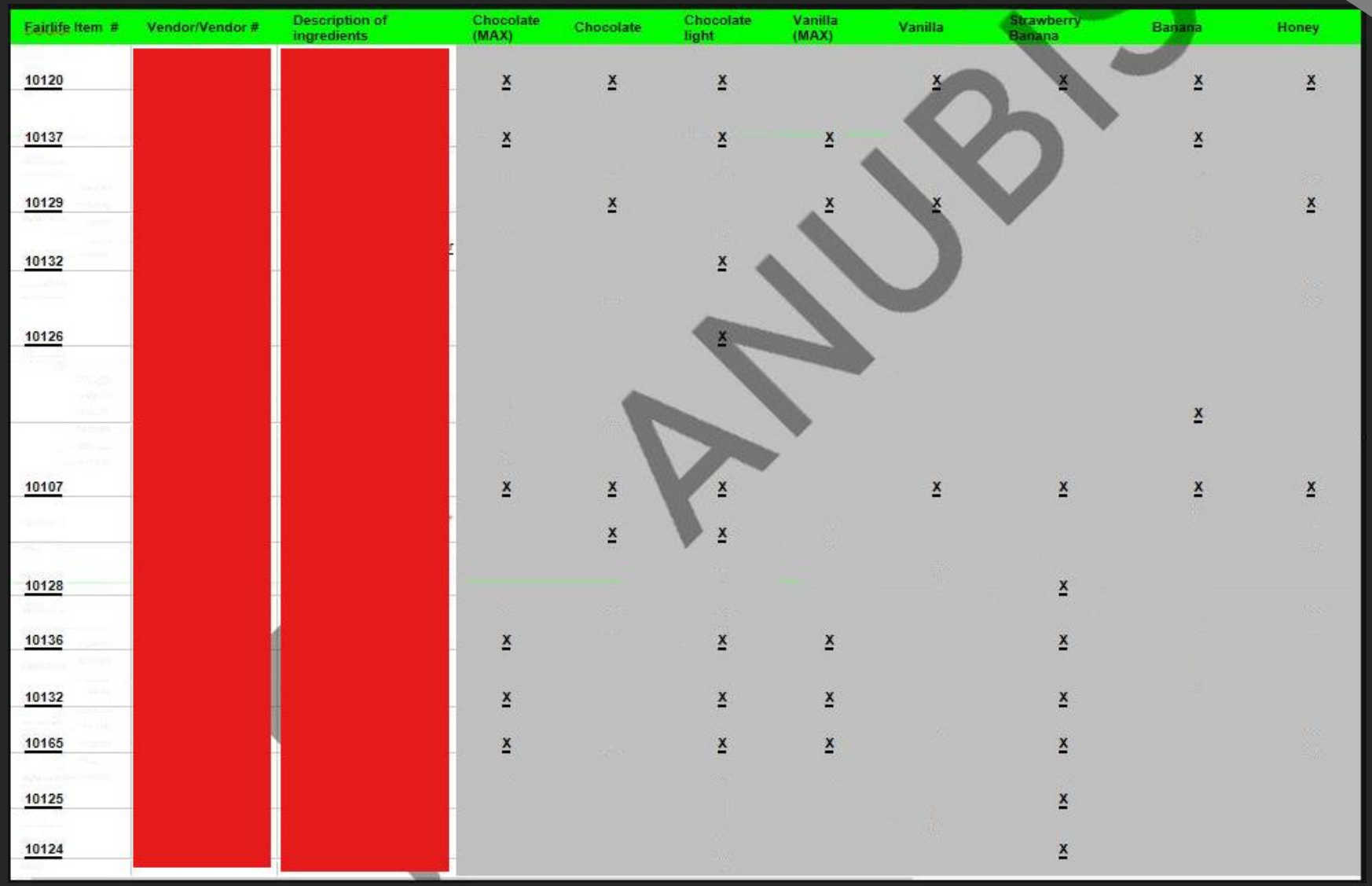
Tetra Pak Dairy & Beverage Systems AB 1 (179)
Staffan Vestberg/ 1834 2013-12-10

INTERNAL DOCUMENT ONLY FOR TETRA PAK SERVICE ENGINEER

Volume handling 3
Function 3
Step conditions based on volume 4
Back up timers 4
Step volumes 5
HP Reclaim and LP Reclaim 10
Reclaim HP (High product content) and reclaim LP (low product content) volumes 17
Signals 18
Signal to Tetra Alsafe 21
Set up menus 22
Set up volume 23
Register setting volume 24
Volume bar graphs 25
Batch target volume 26
Mix phase tuner QT78. 27
Back ground 27
Purpose for mix phase tuner function 27
Function 28
Mix phase volume 28
QT78 settings 29
Capacity selection. 33
AFM selection 33
AFM Cap configuration 34
Cap selection 35
Tank queuing function 36
PID control TIC44 37
Flow control TA Flex homogenizer. 38
Function FC6 38
Pictures for Flow control 39
Flow control when Centrifugal pump 41
Flow control handling in TA Flex 42
Flow control 42
Flow control during water test 45
Fo / PU compensation. 46
Basic function 46
HC Flow 48
Fo compensated temp set point 49
Fo compensated HC temp 50
Flow guards 52
Flow controller alarm 52
HC guard 53
HC Fo guard 53

ANUBIS

Proprietary Industrial Processes



Fairlife Item #	Vendor/Vendor #	Description of ingredients	Chocolate (MAX)	Chocolate	Chocolate light	Vanilla (MAX)	Vanilla	Strawberry Banana	Banana	Honey
10120	[redacted]	[redacted]	X	X	X		X	X	X	X
10137			X		X	X			X	
10129				X		X	X			X
10132					X					
10126					X					
									X	
10107			X	X	X		X	X	X	X
				X	X					
10128								X		
10136			X		X	X		X		
10132			X		X	X		X		
10165			X		X	X		X		
10125								X		
10124								X		

ANUBIS

Proprietary Industrial Processes



Proprietary Industrial Processes



Human Resources Documents

Names, Phone numbers, emergency contacts

Name	Phone #	Emergency Contact
Ad[redacted]	(616[redacted]	Marci[redacted]
Ad[redacted]	(616[redacted]	Jamie[redacted]
Ag[redacted]	(231[redacted]	Sarah[redacted]
Alv[redacted]	(231[redacted]	Dan 2[redacted]
Am[redacted]	(616[redacted]	Autur[redacted]
Ave[redacted]	(815[redacted]	Chad[redacted]
Ba[redacted]	(616[redacted]	Marie[redacted]
Bal[redacted]	(616[redacted]	Violet[redacted]
Bal[redacted]	(616[redacted]	Lucia[redacted]
Bal[redacted]	(616[redacted]	Kristi[redacted]
Ba[redacted]	(989[redacted]	Kasey[redacted]
Ba[redacted]	(231)[redacted]	Kris 2[redacted]
Ba[redacted]	(616[redacted]	Kyle 6[redacted]
Be[redacted]	(616[redacted]	Karen[redacted]
Be[redacted]	(616[redacted]	Dr. Ti[redacted]
Be[redacted]	(231[redacted]	Danie[redacted]
Be[redacted]	(616[redacted]	Sue 6[redacted]
Be[redacted]	(360[redacted]	Jeff 3[redacted]
Be[redacted]	(616[redacted]	Meag[redacted]
Bil[redacted]	(231[redacted]	Bryan[redacted]
Bit[redacted]	(231[redacted]	Jeff 6[redacted]
Bo[redacted]	(231[redacted]	Barba[redacted]
Bo[redacted]	(231[redacted]	Kathy[redacted]
Bo[redacted]	(616[redacted]	Corin[redacted]
Bo[redacted]	(517[redacted]	Fred 9[redacted]
Bra[redacted]	(616[redacted]	Sarah[redacted]
Bro[redacted]	(616[redacted]	Meliss[redacted]
Bro[redacted]	(231[redacted]	Sama[redacted]
Bro[redacted]	(616[redacted]	Hayle[redacted]
Bru[redacted]	(616[redacted]	Laure[redacted]
Bry[redacted]	(231[redacted]	Sue 2[redacted]

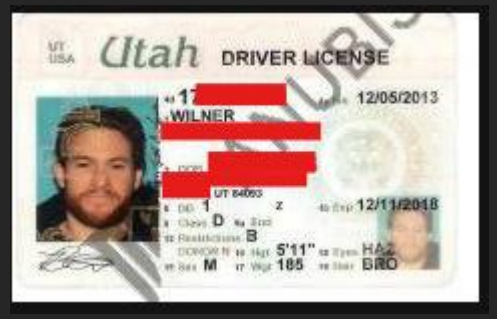
Human Resources Documents

Payroll Information

Reports To Name	Payroll Name	Hire Date	Job Title Description	Annual Salary	New Job Title	change type	% increase scenario 1 (3%)	New Salary	% increase scenario 1 (5%)	New Salary	New Spvr
Schr	Web	01/06/2014	Analytics Manager	$11	Analytics Manager	no change	0	$ 11	0	$ 1	
Schr	Dien	04/10/2017	Channel Manager - WH	$11	Channel Manager - WH	no change	0	$ 11	0	$ 1	
Schr	John	02/19/2018	Director of Commercialization & RGM	$14	Director of Commercializa	no change	0	$ 15	0	$ 1	
Dipa	O'Ke	09/23/2013	National Account Executive	$12	Director, National Accts	promo	0.05	$ 13	0.05	$ 1	
Smit	Wale	02/23/2015	Sales Development Manager	$63	Divisional Sales Manager	promo	0.05	$ 6	0.05	$	
Lobu	Van	07/08/2013	Divisional Sales Manager	$66	Divisional Sales Manager	no change	0	$ 6	0	$	
Lobu	Stree	05/30/2017	Sales Development Manager	$66	Divisional Sales Manager	promo	0.05	$ 6	0.05	$	
Ree	Bish	12/11/2012	Divisional Sales Manager	$79	Divisional Sales Manager	no change	0	$ 7	0	$	
Haw	Now	04/12/2017	Divisional Sales Manager	$86	Divisional Sales Manager	no change	0	$ 8	0	$	
Haw	Harp	04/17/2017	Divisional Sales Manager	$86	Divisional Sales Manager	no change	0	$ 8	0	$	
Haw	Jedd	04/13/2015	Divisional Sales Manager	$90	Divisional Sales Manager	no change	0	$ 9	0	$	
McA	Spot	04/10/2017	Divisional Sales Manager	$91	Divisional Sales Manager	no change	0	$ 9	0	$	
Tayl	Andr	01/03/2017	Sales Development Manager	$59	n/a			$ 7		$	
How	Sam	12/19/2016	Sales Development Manager	$61	n/a			$ 7		$	
How	Ador	08/28/2017	Sales Development Manager	$65	n/a			$ 7		$	
Ree	Nigg	07/03/2017	Sales Development Manager	$65	n/a			$ 7		$	
McA	Tom	10/03/2017	Divisional Sales Manager	$88	National Account Manager	lateral	0.03	$ 9	0.05	$	
Max	Szal	04/24/2012	Divisional Sales Manager	$92	National Account Manager	lateral	0.03	$ 9	0.05	$	
McA	Smit	08/26/2013	Divisional Sales Manager	$97	National Account Manager	lateral	0.03	$ 10	0.05	$ 1	
Dipa	Lars	10/05/2015	National Account Executive	$10	National Account Manager	no change	0	$ 10	0	$ 1	
Dipa	DiFl	10/17/2011	National Account Executive	$11	National Account Manager	no change	0	$ 11	0	$ 1	
Max	Erma	11/06/2013	Divisional Sales Manager	$71	Regional Sales Manager	promo	0.05	$ 7	0.05	$	
Max	Zerr	04/10/2017	Divisional Sales Manager	$86	Regional Sales Manager	title change	0	$ 8	0	$	
Ree	Dunc	08/14/2017	Divisional Sales Manager	$91	Regional Sales Manager	title change	0	$ 9	0	$	
Lobu	Guti	02/02/2014	Divisional Sales Manager	$96	Regional Sales Manager	title change	0	$ 9	0	$	
McA	Edel	01/21/2013	Divisional Sales Manager	$96	Regional Sales Manager	title change	0	$ 9	0	$	
Bisk	Tayl	05/06/2013	Divisional Sales Manager	$98	Regional Sales Manager	title change	0	$ 9	0	$	
Bisk	How	05/06/2013	Divisional Sales Manager	$98	Regional Sales Manager	title change	0	$ 9	0	$	
Bisk	Haw	11/30/2015	Regional Director	$13	Regional Sales Manager	title change	0	$ 13	0	$ 1	

MARKUP

Human Resources Documents





I, Brit, acknowledge that I have read an understand the Fleet Vehicle Expense Policy and Process of fairlife. I agree to adhere Policy in its entirety I understand that if I violate the rules set forth in the Policy, I may liability for the losses to fairlife associated with such violation.

Name: Brit

Signature:

Driver's License Number: NC 28

Driver's License Expiration Date:

Date: 5/21/14







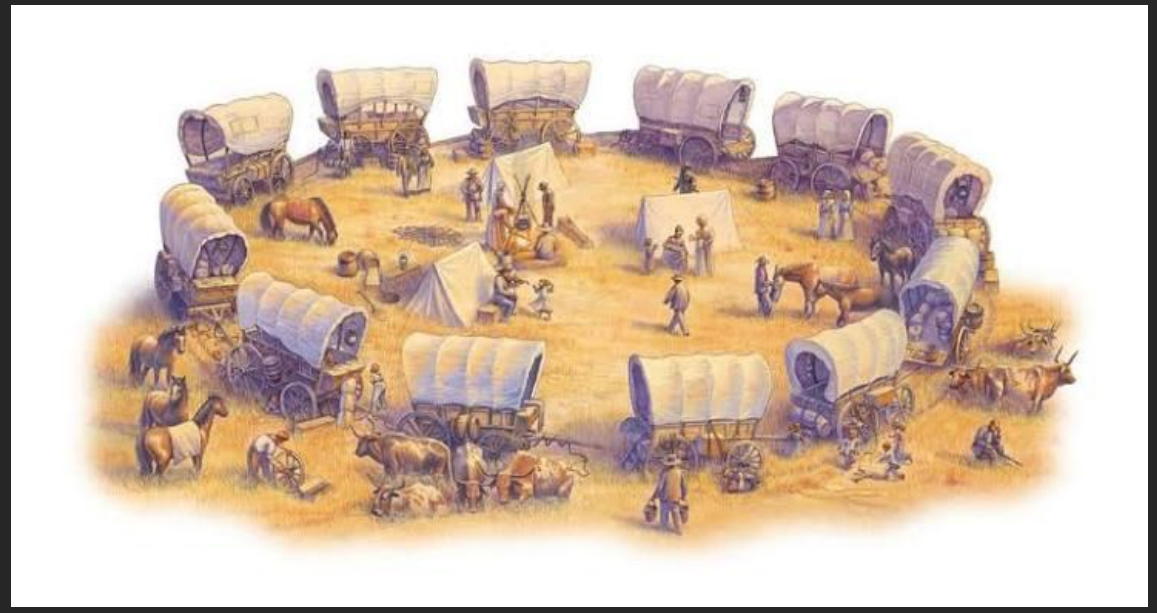
ANUBIS

Agriculture is Vulnerable

- Can your facility withstand 11 days of downtime? Do you have the funds to meet ransom demands?

- Agriculture is actively targeted
  - Perishable supply chain -> immense time pressure

- Deep interdependency among critical infrastructure sectors



Circle the Wagons

CONTACT US

VISIT THE **SC CIC WEBSITE** FOR MORE INFORMATION

HTTPS://SCCIC.SC.GOV/

LDGRADY@SLED.SC.GOV

CYBER@SLED.SC.GOV