



Risk & Compliance Solutions | Webinar

# Artificial Intelligence

## The good, the bad & the ugly

Proprietary and confidential. Do not distribute.



# Today's session



**Chris Gill**

Senior Manager – Maryland  
TruStage™



**Brianda Rojas-Levering**

Risk Consultant – Kentucky  
TruStage™



**Ken Otsuka**

Senior Risk Consultant – Illinois  
TruStage™



→ | **What's on tap?**



# AI is evolving

**Automation** is about setting up a machine to follow a set of predefined rules

**Artificial intelligence (AI)** is about setting up a machine to make its own decisions

AI uses **cognitive functions** we associate with human minds, such as perceiving, reasoning, learning, interacting with an environment, problem solving, and even exercising creativity

**Generative AI** is an AI model that generates content in response to a prompt



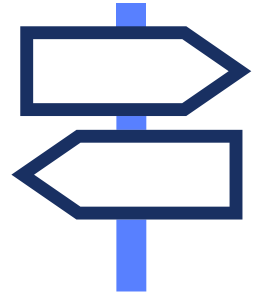
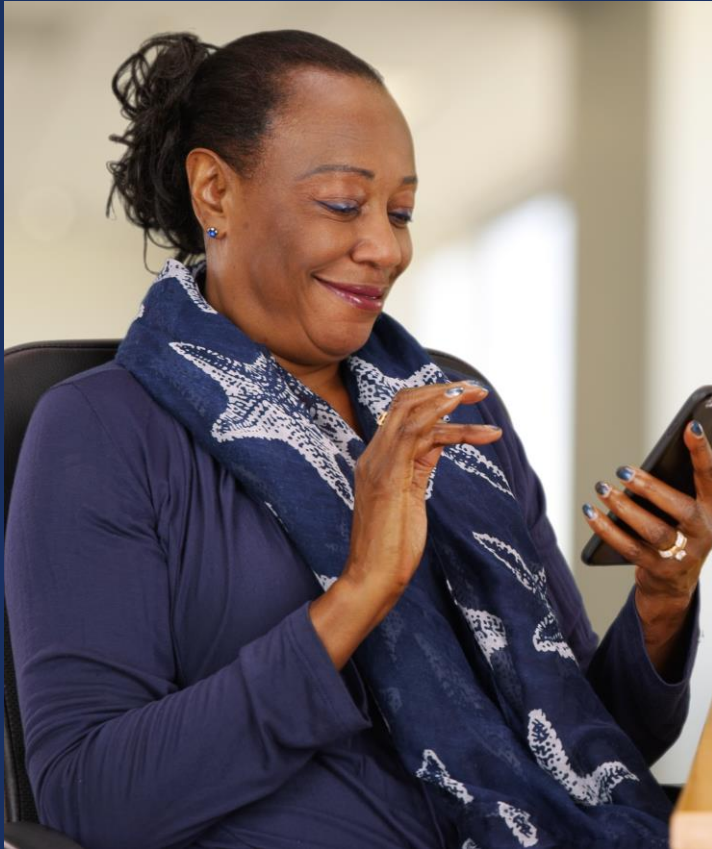


# Evolution of AI

Diagnostic		Predictive		Generative
Why did this happen?		What might happen	What should we do next	How AI can help execute
<ul style="list-style-type: none"><li>Analyze</li><li>Scenario</li><li>Segment</li></ul>		<ul style="list-style-type: none"><li>Pattern</li><li>Forecast</li><li>Model</li></ul>	<ul style="list-style-type: none"><li>Simulate</li><li>Optimize</li><li>Recommend</li></ul>	<ul style="list-style-type: none"><li>Advise</li><li>Create</li><li>Code</li><li>Automate</li><li>Protect</li></ul>

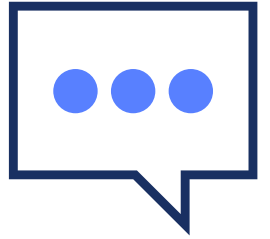
Source: Work, Workforce, Workers Age of Generative AI Report, Accenture, 2024

# Common uses of AI



- Applications
- Fraud monitoring – real-time
- AI-driven perimeter defense (cybersecurity)
- Virtual teller chatbot or other member service solutions
- Content creation
  - Marketing and sales
  - Compliance
  - Human resources
- Talent screening & acquisition
- Predictive analytics

# Building trust in AI



The uncertainty surrounding the emergence of new technologies can often evoke fear. One of the best ways to combat fear is to educate and get people involved, and the companies that do so will have a better chance at creating increased value for themselves and their customers.

Christy Pambianchi, Executive Vice President & Chief Human Resources Officer, Intel

# Understanding the AI value & risks





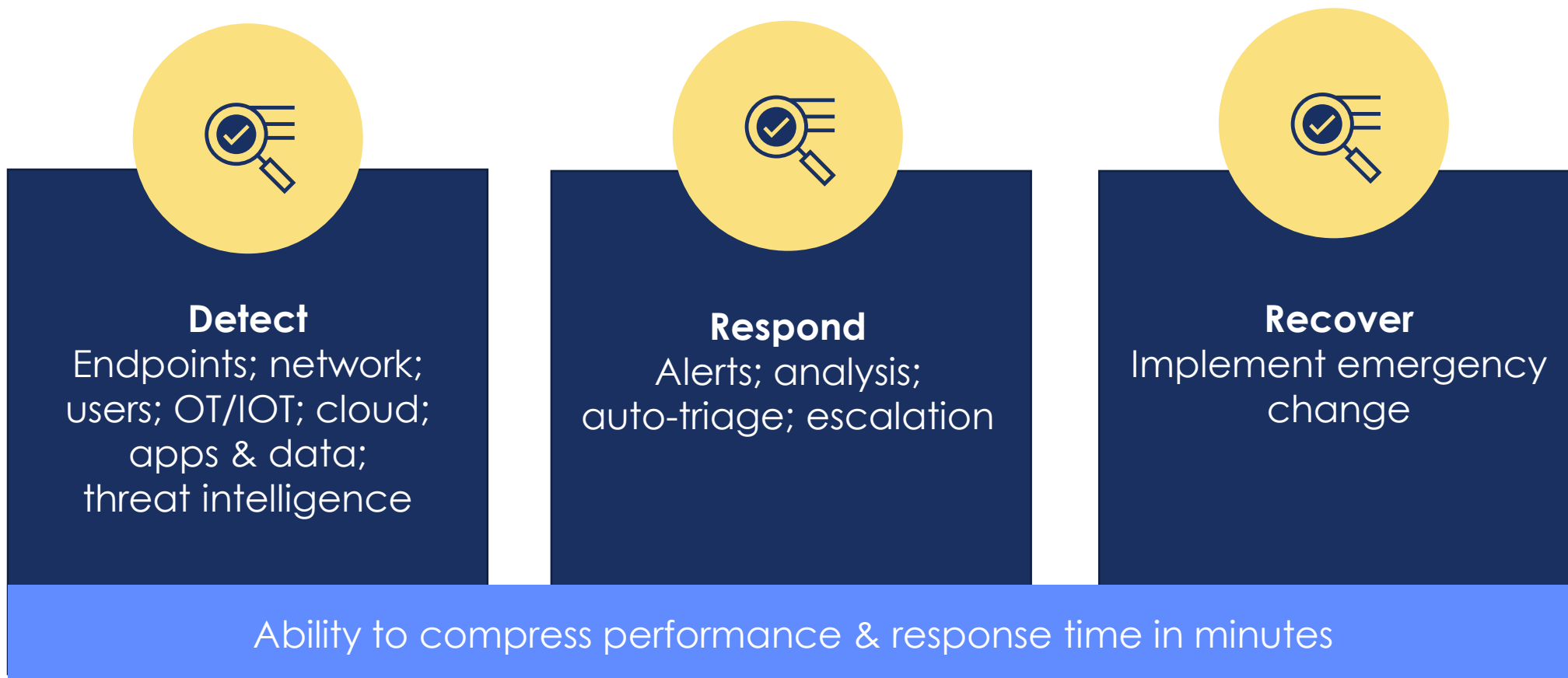


## AI **used to bolster** security and compliance postures with activities like:

- Enhancing cybersecurity defenses
- Third-party compliance & regulatory checks
- Automated security patching
- Incident response & threat containment
- Policy creation



# The **GOOD** Cybersecurity



# The **GOOD** | Real-time fraud monitoring

- Best practice: deploy a real-time fraud monitoring solution leveraging AI and machine learning
- Machine learning is a component of AI
- AI leverages data and algorithms to flag potential fraudulent transactions
- Learns from historical data
- Learns and adapts to new and changing fraud patterns

## **AI's role**

- Anomaly detection
- Machine learning modules
- Behavior analytics
- Network analysis
- Real-time decisioning
- Fraud pattern recognition
- Reduces false positives
- Adaptive security
- Automation

# The **BAD** Generative AI risks



- **Generation of phishing emails** - it can produce well-crafted phishing emails in multiple languages without common warning signs
- **Creation of malware** - due to its ability to generate code in many languages, it can create malware to detect sensitive user data, hack entire computer systems, or scan email accounts
- **Privacy issues** – it retains the user's sensitive info, which can pose a data threat if it gets misused
- **Inaccurate data or missing information** – Generative AI, like ChatGPT, is trained on vast amounts of data, and in the case of inaccurate data or missing information, the responses will reflect those issues
- **Biased content** – answers have been provided that are not aligned with cultural diversity
- **Plagiarism** – text can be generated that is similar to existing content based on training data patterns.



# The **BAD** Phishing

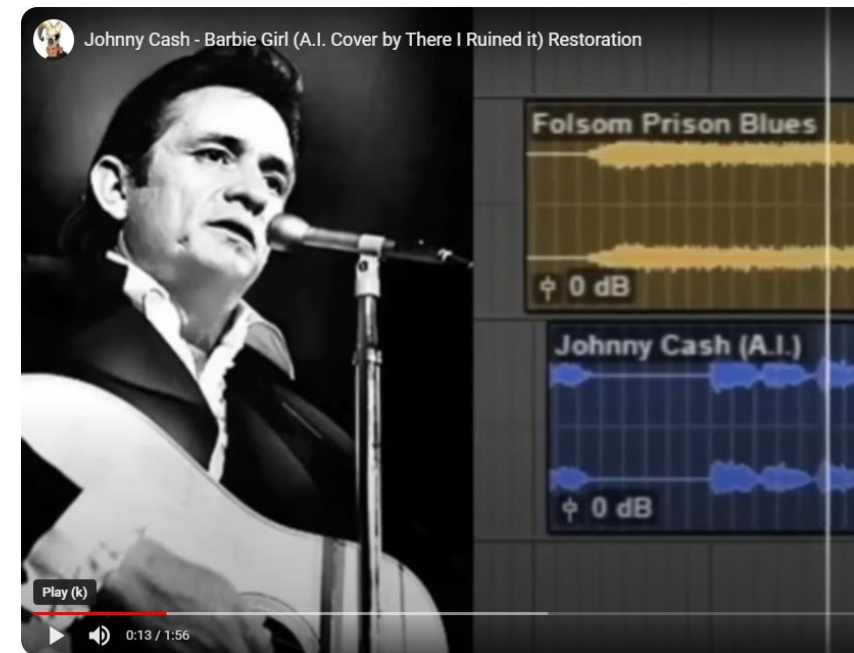
- Generative AI can be used for nefarious purposes
- Craft well-written phishing emails
- ChatGPT rules prohibit its use for fraudulent purposes
- Users circumvent restrictions with the right prompts
  - Use "jailbreaks" to circumvent restrictions
  - Engage similar chatbot services – such as WormGPT or FraudGPT - to write malicious software without security prohibitions



# The **BAD** Deepfake imposter scams

- Fraudsters obtain images and voice samples from social media, videos, or cold-calling to record a voice
- Convincing deepfakes are developed to look and/or sound like someone an individual or employee knows
- Think **business email compromise, fraudulent instruction, and even video banking scams**
- Conventional security technologies and member identification protocols are designed to identify impostors - not recognize altered or recorded voices or digitally enhanced and manipulated videos

Combining generative AI's language processing abilities with visual deepfake and/or voice recreation technologies





What tips do you suggest to  
identify and combat deepfakes?

Michaele - Pennsylvania





Should an organization rely on AI for hiring decisions? Are there any known pitfalls for using AI concerning HR decision making?

Sonjia - Virginia

# HR & talent acquisition risks



## **Bias**

If the human input into the system is biased, it will be reflected in the AI's decision-making process.

gender, race, age, or disability



## **Transparency**

Challenging to ensure that hiring decisions are fair and based on merit rather than other factors.



## **Exclusion**

if an AI system is trained on data that reflects your historical hiring patterns, it may perpetuate these patterns.

# Compliance & regulatory concerns

- Unregulated atmosphere
- Evolving and unknown regulatory requirements
- Trademarked works
- Reputational damage
- Regulatory penalties
- Compliance challenges

Many grapple with the ethical and practical issues brought up by the use and misuse of AI technologies.

2024 is shaping up to be a pivotal year for both AI development and regulatory changes





## Why is AI subjected to compliance regulations?

- Ethical & legal standards
- Trust & transparency
- Avoiding harmful outcomes
- Ensuring accountability

# The **UGLY** Data privacy concerns

- Generative AI takes as much as it gives, meaning the quality of future results relies on the information entered into the system to train it
- It absorbs that knowledge and ensures that it is accessible to anyone who uses the tool going forward
- Employees haphazardly using third-party software
- Failure to ensure that sensitive company or personal information isn't inadvertently disclosed

**43%** of working professionals have used generative AI tools to complete tasks at work.

**68%** hadn't told their bosses.

Fishbowl Insights, 2/1/2023

a social network where professionals come to discuss topics about work-life

# Data privacy & AI



- **Robust policies:** Develop clear and comprehensive policies specifically addressing the use of AI. Policies should cover the sharing of sensitive information, data handling, and appropriate use of AI tools.
- **Training:** Provide training to employees on the responsible and secure use of AI. Make sure all staff understands the potential risks, how to interact safely, and what information should not be shared.
- **Regular auditing:** Conduct regular audits to monitor AI interactions and ensure compliance with data privacy policies. This can help identify any potential breaches or misuse.
- **Encryption:** Ensure that data transmitted between employees and AI is encrypted, protecting it from unauthorized access during transmission.

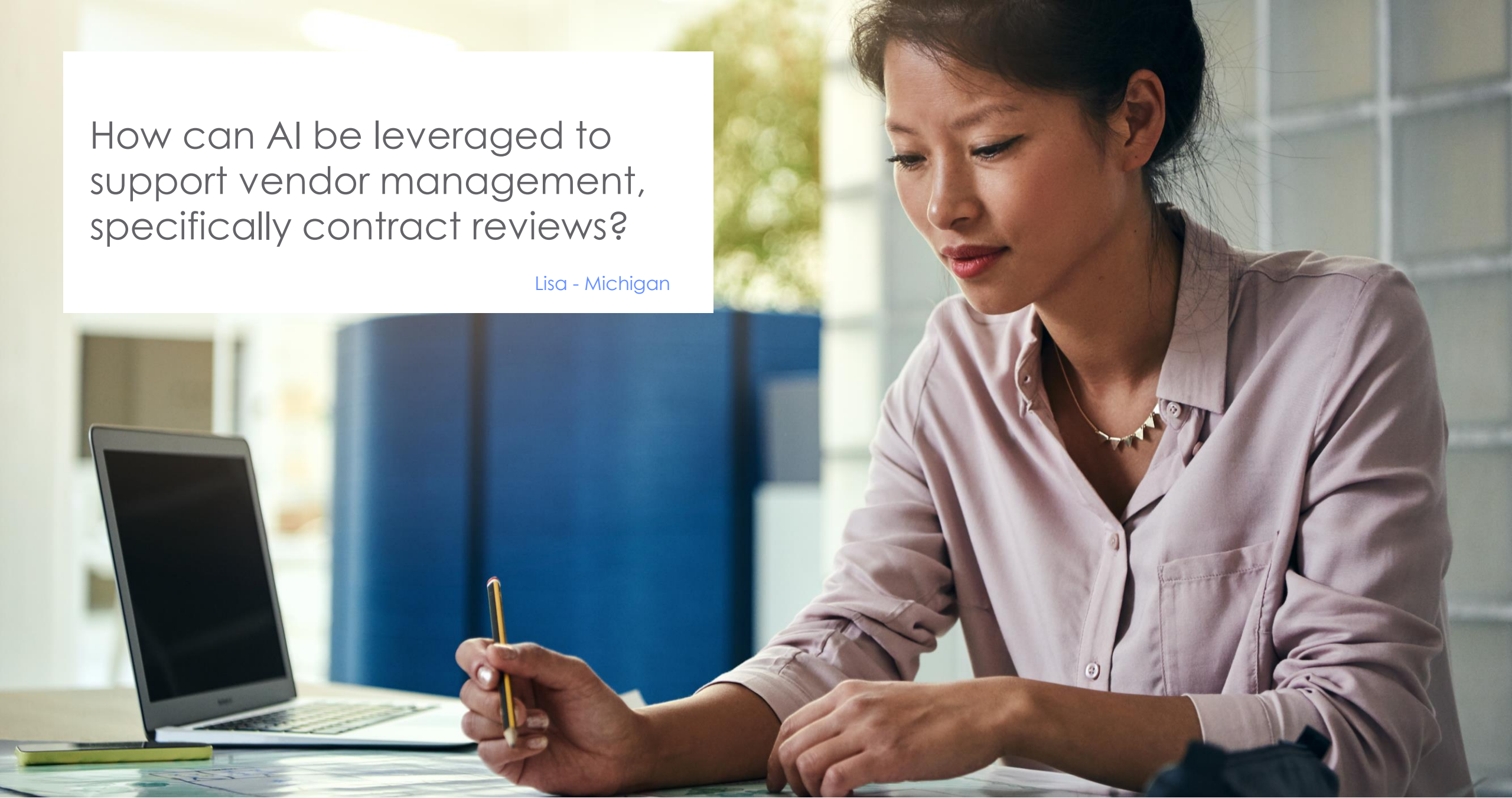
AI systems require volumes of data that can pose significant data privacy risk. AI models that are used to analyze customer or user behavior, for example, may need access to sensitive personal information.

GenAI tools may also share user data with third parties and service providers, potentially violating data privacy laws.



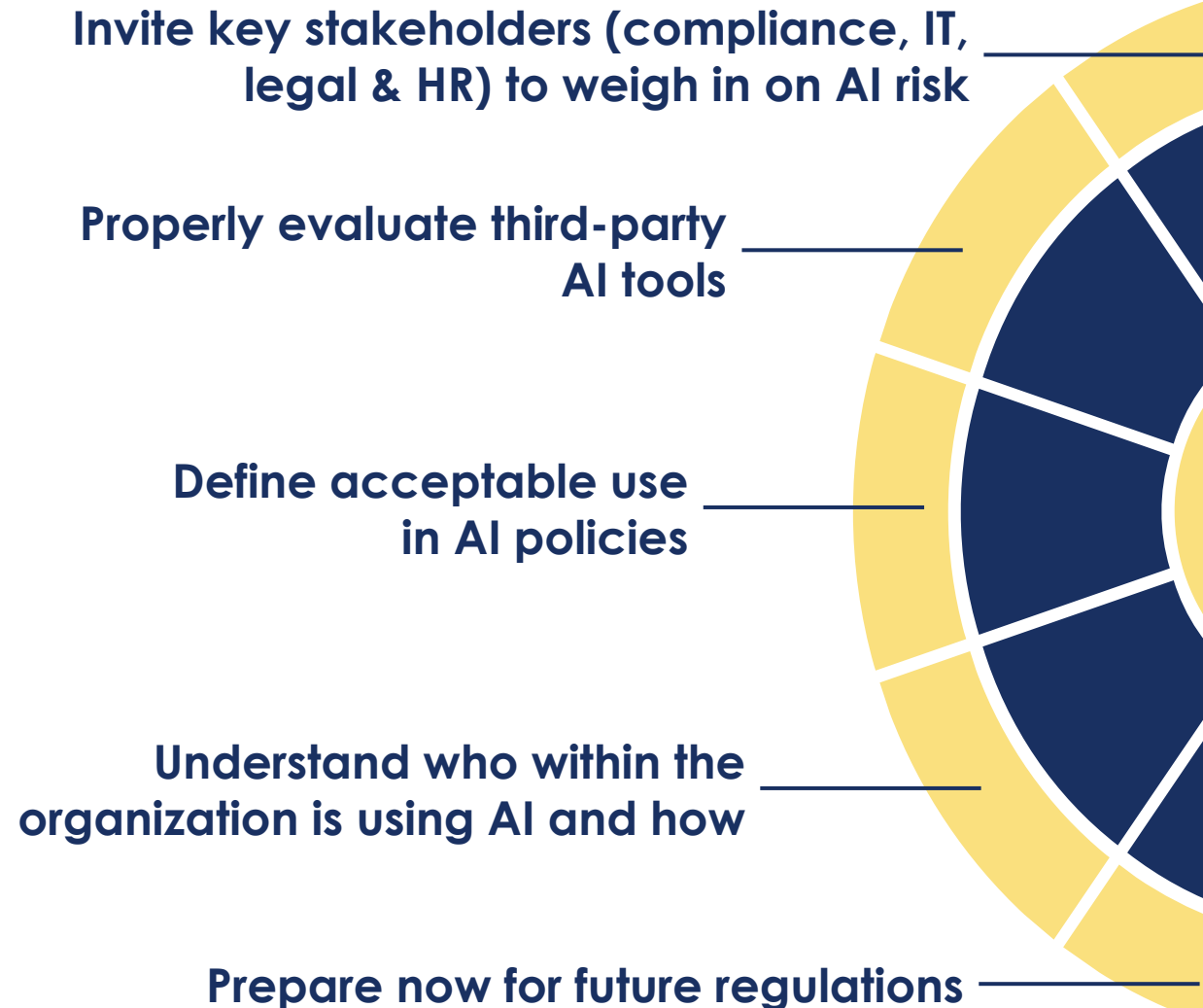
# How can AI be leveraged to support vendor management, specifically contract reviews?

Lisa - Michigan





## Organizational steps to take to navigate AI





**With proper guardrails in place, artificial intelligence and generative AI can unlock innovative use cases for businesses and speed up, scale, or improve existing ones.**



# Risk resources

## Business Protection Resource Center [www.trustage.com/bprc](http://www.trustage.com/bprc)

- RISK Alerts – warning | watch | awareness
- Loss prevention library  
- risk overviews, checklists & whitepapers
- Emerging risks outlook
- Live webinars, risk forums & office hours
- On-demand learning & interactive training modules

“Great webinars - serious, important information delivered in a relaxed, ‘we’re among friends’ way.”

\$9B credit union



### New account fraud

Risk overview

Fraudsters often use consumers' personally identifiable information (PII) that is compromised in data breaches to open new fraudulent accounts at credit unions. While fraudsters may open fraudulent accounts in-person, they prefer to use the online channel as it provides a cloak of anonymity.

**Primary fraud risks**


Two primary fraud risks that credit unions must consider when offering online account opening and funding:

- Opening an account under someone else's identity with the intent to commit fraud, and
- Funding the account using a fraudulent method, such as ACH debit, and withdrawing the funds prior to the ACH item being returned unpaid.

In both scenarios, criminals prefer the anonymity and speed of online channels, allowing them to operate freely. Additionally, they have the ability to adapt to fraud controls at a much faster pace than in-person.

**New account fraud insights**

- New account fraud is generally defined as fraud that occurs within the first 90 days after an account is opened; the accounts are often opened solely to commit fraud.
- Savvy financial criminals frequently wait more than 30 days before making a fraudulent deposit, or they will make small deposits and withdrawals in the first month to establish a pattern.
- Perpetrators sometimes make their deposits on a Friday or Saturday prior to a banking holiday to give them a longer period to withdraw the funds.



### RISK Alert

Actionable insights for bond policyholders

Awareness Watch Warning

**Deepfake imposter scams introduce new fraud risks**

By adopting images and voice samples from social media, videos, or cold-calling to record a voice, fraudsters can make convincing deepfakes that look and/or sound like someone an individual or employee knows. Combining generative AI's language processing abilities with visual deepfake and voice recreation technologies, there are significant risks for financial institutions due to the heightened level of sophistication to fraud attempts.

**Alert details**

A significant challenge facing financial institutions today is that methods commonly used to prevent fraud, such as phone or video calls, are now being used by criminals to perpetrate fraud using deepfakes. Advanced applications and technology allow the fraudster to be off camera while the app fully animates the deepfake image on screen.

Deepfakes – often intentionally distorted videos, images, and audio recordings – have been so convincing that bad actors have already used them in social engineering attacks for financial gain. Social engineering frauds using deepfake technology are a new challenge for credit unions as conventional security technologies and member identification protocols are designed to identify imposters – not recognize altered or recorded voices or digitally enhanced and manipulated videos.

Even though some credit unions have pivoted to the use of photographs or “selfies” with government-issued ID's as well as the adoption of voice recognition software for member identification purposes, imposters have been able to use deepfake technologies to successfully bypass these new protocols.

Credit unions may be affected by deepfakes in several ways:

- exploiting member onboarding processes
- creating fraudulent accounts, counterfeit payment or transfer requests
- impersonating key credit union or third-party personnel
- mimicking job candidates


Unfortunately, it appears that every time risk mitigation techniques are tightened up, fraudsters seem to find a workaround.

**Share with:**

- Branch operations
- Executive management
- Front-line staff/tellers
- Human resources
- IT
- Member services/new accounts
- Risk manager
- Transaction services

**Facing risk challenges?**

Schedule a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.




Risk & Compliance Solutions | Presentation

## Emerging risks outlook

Rethinking protection in an era of uncertainty

Proprietary and confidential. Do not distribute.







# Contact us

**800.637.2676**

- [riskconsultant@trustage.com](mailto:riskconsultant@trustage.com)
- [Ask a risk manager interactive form](#)
- [Schedule a 1:1 risk consultation](#)
- [Report a risk or scam](#)



# Thank you.

**Contact**

**[riskconsultant@trustage.com](mailto:riskconsultant@trustage.com)**

**800.637.2676**

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this presentation/publication, nor does it replace any provisions of any insurance policy or bond.

TruStage™ is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions, and exclusions.