

LET'S TACKLE
COMPLIANCE
TOGETHER

InfoSight



A FREE Resource for
Affiliated Credit Unions

Business Continuity means asking "What if?"
questions and creating plans to address them.



Like, What if your member data becomes compromised?
Are you prepared? **RecoveryPro** can help!

League InfoSight Resources

Fraud Channel and MORE!

LeagueInfoSight

Emma Nelson

Relationship & Regulatory Compliance
Manager

Emma.Nelson@LeagueInfoSight.com

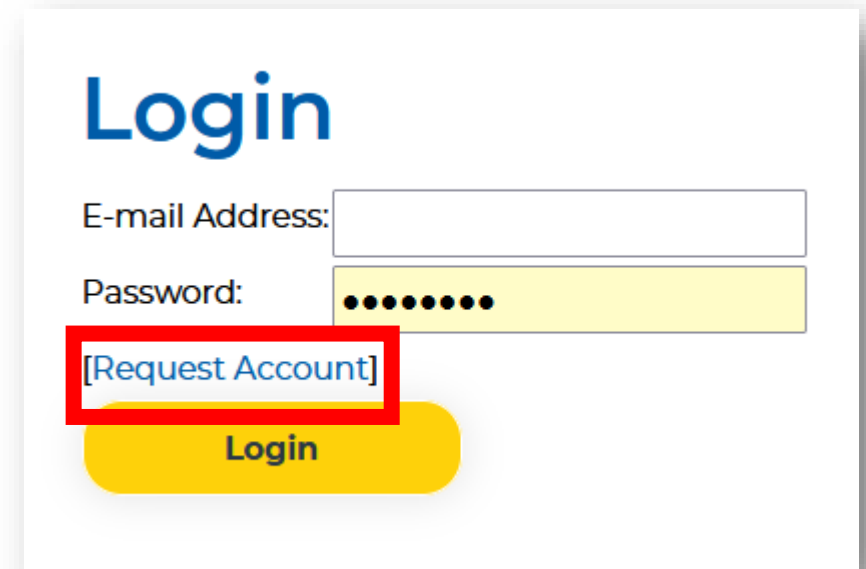
Glory LeDu

CEO of League InfoSight
CEO of CU Risk Intelligence

Glory.LeDu@LeagueInfoSight.com

Where can I find out if I have access to InfoSight?

- Access to InfoSight is through your League/Association website! As a benefit of membership, you will typically find a link under Compliance or Member Resources!
- If you don't have access, you can typically request access or an account directly from the login screen.
- You can also go directly to your League/Association's InfoSight page from here:
 - <https://www.leagueinfosight.com/states>

A screenshot of the InfoSight login interface. It features a white background with the word "Login" in large blue font at the top. Below it are two input fields: "E-mail Address:" with a white text box, and "Password:" with a yellow text box containing ten black dots. A blue link "[Request Account]" is positioned below the password field and is highlighted with a red rectangular border. At the bottom of the form is a yellow rounded button with the text "Login" in black.

Who should use InfoSight?

- **Compliance Staff**
- **Everyone Else!** InfoSight is **NOT** just for the Compliance Officer! Compliance touches every area of the credit union and InfoSight can provide information for:
 - Front line staff
 - Human Resources
 - Loan Officer
 - Board & Volunteers
 - Executive Staff
 - Marketing
 - Collections
 - Lending
 - And MORE!
- There is no limit on the number of users that can access the system!



Compliance Topics

Accounts

ACH/Electronic Payments

Advertising

Bank Secrecy Act

Bankruptcy and Collections

Board Responsibilities

Employment

Field of Membership

Fraud

Investment

Loans and Leasing

Records Retention

Security

Tax Issues

Welcome, Glory

Topics of Interest



- Bankruptcy and Collections
- Foreclosure (Michigan)
- Garnishment (Michigan)
- Investment
- Loans and Leasing

Recently Visited Pages

- InfoSight Listing by State
- Backup Withholding
- Accounts
- Elder and/or Vulnerable Adult Protections
- Security
- Internal Controls and Fraud Prevention
- Current Expected Credit Loss (CECL)

Credit Union Tools

- **NEW!** The 2024 Q2 Compliance Update Video is now available!!
- Help Protect Your Elder Members with the Trusted Contact Toolkit



Compliance Calendar

September, 2024

- September 2nd, 2024: Labor Day - Federal Holiday
- September 16th, 2024: CFPB – Registry of Nonbank Covered Persons Subject to Certain Agency and Court Orders
- September 23rd, 2024: Department of Labor (DOL) – Investment Advice Fiduciary

October, 2024

- October 1st, 2024: NACHA – Fraud Return Reason Code

November, 2024

- November 28th, 2024 - November 29th,

Collaborative Partners

Governance, Risk and Compliance Solutions

CU Risk Intelligence offers a full suite of GRC solutions including auditing and reporting, risk assessments, loan review services and more!

- ComplySight
- AffirmX
- Credit Union Vendor Management



Recently Updated



August 2024 - RISK Alerts

New **RISK Alerts** are now available from TruStage:

- Corporate check fraud reported (8/8/2024)
- ACH transactions risk overview (8/2/2024)
- Card payment fraud / booster payments (8/2/2024)
- ODFI of debits/online deposits (8/2/2024)
- Wire transfer risk overview (8/2/2024)

July 2024 - Employment

Changes have been made to the Expedited Funds Availability – Regulation CC topic in the Accounts channel. Availability

Resources



A - Z Listing

Account Insurance Estimator

All Newsletters

Check Deposit Notice Generator

Collaborative Tools

Compliance Calendar

Compliance Videos

CU PolicyPro

CUNA e-Guide

FAQs

Federal Regulations List

InfoSight Listing by State

Required Compliance Training

RISK Alerts

- Easy-to-Understand Summaries and Information
- Customizable Dashboard
- Checklists
- State-Specific Content
- Links to Laws, Regulations, and additional Resources
- RISK Alerts
- Videos
- Compliance Calendar
- FAQs (over 850)
- Check Deposit Notice Generator
- Account Insurance Estimator

Currency Transaction Reports

Last Reviewed: November 2023

There are several reporting requirements for credit unions and other financial institutions under the BSA. Among these requirements is the Currency Transaction Report (CTR), must be electronically filed at the BSE E-Filing System Website.

All financial institutions, including every credit union, must file a currency transaction report (CTR) on each deposit, withdrawal, payment, transfer or other transactions involving currency (cash) of more than \$10,000.00. If multiple transactions are by or on behalf of any person, the credit union must aggregate transactions and report them as one transaction if the total exceeds \$10,000.00. If deposits are made at night or over a weekend or holiday, that transaction must be treated as if it was made on the next business day.

Summary

Checklist

FAQs

Laws & Regulations

Additional Resources

InfoSight Listing by State

- Alabama
- Alaska
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland/District of Columbia
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey



Fraud Introduction

Last Reviewed: August 2024

Financial institutions must implement measures to prevent, detect, and deter fraud to mitigate losses. Credit unions are also expected to help members against fraud. It is critical to stay aware of fraud trends, educate credit union employees and members, and implement proper anti-fraud measures.

Overview +

Common Fraud Scams +

Reporting Fraud +

Top Reported Fraud +

Warning Signs +

Laws & Regulations +

Additional Resources +

Model Policies +

Fraud Topics:

The following topics are covered in the Fraud Channel:

- **Fraud Introduction**
- Check Fraud
- Cyber-Enabled Fraud
- Elder and/or Vulnerable Adult Protections
- Internal Fraud
- Risk Management
- **Training - Credit Union Fraud Symposium**
- Wire Transfers



Check Fraud

Last Reviewed: August 2024

Check Fraud is still prevalent among fraudsters. Financial institutions and their members should be aware of check scams and how to avoid falling victim.

Cashier's Check Fraud



Mail Theft-Related Check Fraud



Additional Resources



 Print Additional Resources

Check Fraud: Additional Resources

- [Check Deposit Notice Generator](#)
- [FinCEN Alert on Check Fraud Schemes](#)
- [OCC Avoiding Cashier's Check Fraud](#)
- [United States Postal Inspection Service \(USPIS\) Hotline](#)

Model Policies



Cyber-Enabled Fraud

Last Reviewed: August 2022

Additional information on cybersecurity and cybersecurity resources can be found in the [Security Channel](#).

Cybercrime



Phishing Attacks



Additional Resources



Model Policies



Cybersecurity

Last Reviewed: August 2024

Credit unions must be vigilant in preparing and protecting themselves against the many threats (physical and virtual) in the cyber world. It's critical for the credit union to research and employ technology and resources to defend against the evolving threats.

Summary



Automated Cybersecurity Evaluation Toolbox (ACET)



Cybersecurity Assessment Tool



Additional Resources



Model Policies



Cybersecurity Resources

Below is a compilation of topics and tools within our products addressing various aspects of cybersecurity. These resources cover general cybersecurity principles and the regulatory requirements for prevention, control, and effective response.

InfoSight

- [Cybersecurity](#)
- [Data Breach](#)
 - Member Notification and Content Notice
 - Media Response Components
 - State Considerations
- [Security Program for Credit Unions](#)
 - NCUA Notification Requirements
 - Information Security Program Requirements

CU PolicyPro

- [Policy 4120 – Information Security](#)
- [Policy 4125 – Incident Response](#)

RecoveryPro

- Section 1600: Cyber Incident Response Process
 - [Procedures for detecting, containing, and recovering from Cyber Attacks](#)
 - [Cyber Incident Reporting](#)
 - [Communications Template](#)
 - [Cyber Incident Planning Recommendations](#)
 - [Cyber Event - Threat Assessment](#)

Security Program For Credit Unions

Last Reviewed: August 2024

Part 748 of the NCUA Rules and Regulations requires each federally-insured credit union develop a comprehensive written security program (including administrative, technical, and physical safeguards appropriate to their size, complexity, and the nature and scope of their operations) within 90 days of the date it is insured by the National Credit Union Share Insurance Fund (NCUSIF). The security program and associated procedures will be evaluated during examinations by the NCUA or state credit union regulator.

Summary



Physical Security



Information Security



Checklist



FAQs



Laws & Regulations



Additional Resources



Model Policies









- CU PolicyPro is offered in many states as a member benefit for free or deeply discounted and helps to further strengthen the credit union's compliance efforts.
- Provides access to 230+ completely developed model policies and procedures, researched and written by Credit Union experts.
- Provides sample forms, documents, and other resources too!
- Designed for federal regulatory compliance.
- Complete Policy Management System including auditing tools, updated information, secured distribution of policies, and policy review assignment capabilities.
- **Nationwide**
 - 3400 + credit unions are registered for CU PolicyPro
 - Credit Unions from all 50 states are using CU PolicyPro



Logged in as: Glory LeDu (Staff) Access Level: Admin Change Password

Content

Function	CU PolicyPro	RecoveryPro
View Model Content		
View Published Documents		
Edit Content		

Latest News

The last **RecoveryPro** content update included the addition of a comprehensive **Cyber Incident** section, developed to address NCUA's heightened emphasis on cyber events and Business Continuity Planning (BCP). The following recorded webinar takes a deep dive into the new content, including procedures for detecting, containing, and recovering from cyberattacks, along with communication strategies for notifying key stakeholders.

[Cyber Incident Content Overview Recording](#)

Assignments

There is nothing currently assigned to you.

- Model content is located directly from the dashboard!

- Trainings are offered on new/hot topics.
- Monthly newsletters are distributed with relevant content updates/information.

- 230+ **Model Policies and Procedures** organized into 11 chapters.

View CU PolicyPro Model Policies

Expand All | Collapse All

Chapter 1000: Administrative ▶

Chapter 2000: Operations ▶

Chapter 3000: Accounting ▶

Chapter 4000: Security ▶

Chapter 5000: Asset/Liability Management ▶

Chapter 6000: Investments ▶

Chapter 7000: Lending ▶

Chapter 8000: Other Real Estate Owned (OREO) ▶

Chapter 9000: Federal Regulations ▶

Chapter 10000: Records Retention ▶

Chapter 11000: Fair Credit Reporting Act ▶

Chapter 1000: Administrative ▼

- Policy 1100: Credit Union Culture and Governance
 - 1100.10: Organization
 - 1100.11: Field of Membership
 - 1100.12: Board of Director's Duties
 - 1100.13: Compensation, Reimbursement, and Indemnification
 - 1100.14: Bond and Insurance Coverage
 - 1100.15: Education and Volunteer Training Guidelines
 - 1100.16: Strategic Planning
 - 1100.17: Audits
 - 1100.18: Legal Counsel
 - 1100.19: Code of Ethics and Diversity
- Policy 1230: Regulatory Compliance
 - 1230.10: Complaint Process for Federally Chartered Credit Union
 - 1230.11: Complaint Process for State-Chartered Credit Union
- Policy 1240: Enterprise Risk Management
- Policy 1500: Staffing and Human Resources
 - 1500.10: Whistleblowing Protection
 - 1500.11: Nepotism
 - 1500.12: Equal Opportunity Statement
 - 1500.13: Political Contributions
 - Policy 1500.14: Payroll
- Policy 1516: COVID-19 Vaccination, Testing and Face Covering Policy
- Policy 1520: Succession Planning
- Policy 1530: Employee Use of Social Media
- Policy 1531: Credit Union Use of Social Media
- Policy 1615: Privacy and Confidential Information
- Policy 1620: Conflict of Interest
- Policy 1645: Fraud

Viewing CU PolicyPro Model Policy: "Bank Secrecy Act/Anti-Money Laundering Program" (Policy 2110)

Print | Return to Model Policy List | Switch to Admin View

Policy 2110: Bank Secrecy Act/Anti-Money Laundering Program

Revised Date: 1/3/2024

Model Policy Revised Date: 01/03/2024

General Policy Statement:

[[CUname]]'s (Credit Union) comprehensive Bank Secrecy Act (BSA) / Anti-Money Laundering (AML) Program will include internal policies, procedures, and controls designed to comply with the USA PATRIOT Act of 2001 (PATRIOT Act), the BSA, the Currency and Foreign Transactions Reporting Act, OFAC rules, the Anti-Money Laundering Act of 2020, and all related laws and regulations in order to combat money laundering, terrorist financing, tax evasion and other financial crimes.

Definitions:

1. **Money Laundering.** Money laundering is the criminal practice of processing "dirty" money through a series of transactions in order to "clean" the funds so that they appear to be proceeds from legal activities. It may not involve currency (cash) at every stage of the laundering process, and generally involves three independent steps (that can occur at the same time):

A. **Placement:** Structuring currency deposits in amounts to evade reporting requirements, or commingling currency deposits of legal and illegal activities. Examples:

- Large number of deposits below the reporting threshold.
- Depositing a refund check from a canceled vacation package or insurance policy.
- Buying a series of monetary instruments that are collected and deposited at another location.

B. **Layering:** Moving funds around the financial system, often in a complex series of transactions. Examples:

- Exchanging monetary instruments for larger or smaller amounts.
- Wiring or transferring funds to and through numerous accounts in one or more financial institutions.

C. **Integration:** Creating the appearance of legality through additional transactions. Example:

- The purchase and resale of real estate or other assets.

RecoveryPro

- RecoveryPro is an online system which guides credit unions through the creation, maintenance, and testing of robust business continuity plans (BCPs).
- Model content, checklists, worksheets, business process summaries and more are provided and can be completely customized to your credit union's operations.
- Uses the same technology as CU PolicyPro, therefore has a complete content management system including auditing tools, updated information, secured distribution of policies, and policy review assignment capabilities.
- Pricing is based on asset size and is heavily discounted for affiliated credit unions (as low as \$249 annually)!



View RecoveryPro Model Content

Expand All | Collapse All

1000: Incident Management ▶

2000: Business Continuity Plan ▶

3000: Systems Recovery ▶

4000: Plan Validation and Maintenance ▶

5000: Business Impact Analysis ▶

6000: Risk Assessment ▶

7000: Business Continuity Policies ▶

- 2700: Business Process Summaries
 - 2700-A: Business Process Summary - BLANK TEMPLATE
 - 2710: Finance & Accounting
 - 2710.10: Business Process Summary - Regulatory Reporting (if not included in 2710.15)
 - 2710.11: Business Process Summary - Accounts Payable
 - 2710.12: Business Process Summary - Annual Budget (if not included in 2710.15)
 - 2710.13: Business Process Summary - Financial Reporting
 - 2710.14: Business Process Summary - GL Reconciliation
 - 2710.15: Business Process Summary - Board Reporting (if not included in 2710.10-2710.14)
 - 2720: Human Resources
 - 2720.10: Business Process Summary - Payroll
 - 2720.11: Business Process Summary - HR Functions
 - 2720.12: Business Process Summary - Training (if not included in 2720.10-2720.11)
 - 2730: Information Technology
 - 2730.10: Business Process Summary - IT Security
 - 2730.11: Business Process Summary - Manage IT Infrastructure
 - 2730.12: Business Process Summary - Manage Telecommunications
 - 2730.13: Business Process Summary - IT Support
 - 2740: Lending
 - 2740.10: Business Process Summary - Consumer Lending
 - 2740.11: Business Process Summary - Indirect Lending
 - 2740.12: Business Process Summary - Loan Servicing
 - 2740.13: Business Process Summary - Member Business Loans
 - 2740.14: Business Process Summary - Mortgage Lending
 - 2750: Management-Administration
 - 2750.10: Business Process Summary - Communications
 - 2750.11: Business Process Summary - Incident Management
 - 2750.12: Business Process Summary - Decision-Making Authority
 - 2750.13: Business Process Summary - Facilities Management
 - 2750.14: Business Process Summary - BSA
 - 2750.15: Business Process Summary - Administer Business Continuity Plans
 - 2750.16: Business Process Summary - Manage Liquidity/Investments
 - 2750.17: Business Process Summary - Regulatory Compliance
 - 2750.18: Business Process Summary - Vendor Management
 - 2760: Marketing
 - 2760.10: Business Process Summary - Manage Social Media
 - 2760.11: Business Process Summary - Marketing Campaigns
 - 2760.12: Business Process Summary - Marketing Events
 - 2770: Member Service
 - 2770.10: Business Process Summary - Check Processing
 - 2770.11: Business Process Summary - Member Transactions

- 1500: Incident Management Process
 - 1510: Notification/Escalation
 - 1520: Command Center Establishment
 - 1530: Incident Monitoring
 - 1540: Decision Making
 - 1550: Communications
 - 1551: Communications Templates
 - 1560: Event/Incident Postmortem Activity
- 1600: Cyber Incident Response
 - 1610: Introduction
 - 1620: Process Flow Chart - Cyber Incident
 - 1630: Response Team Roles & Responsibilities
 - 1640: Cyber Incident Contacts
- 1650: Cyber Incident Response Process
 - 1651: Detection and Analysis
 - 1652: Containment, Eradication & Recovery
 - 1653: Post Incident Activity
 - 1654: Cyber Incident Reporting
 - 1655: Member Notifications
 - 1656: Communications
 - 1657: Cyber Incident Communications Template
- 1660: Cyber Incident Resources
 - 1661: Cyber Incident Response Wallet Cards
 - 1662: Common Types of Cyber Incidents and Response Planning
- 1670: Cyber Incident Resources - Appendix
 - 1671: Cyber Incident Scenario Examples
 - 1672: Cyber Incident Planning Recommendations
 - 1673: Full Cyber Incident Life Cycle


Welcome back, Christopher!

Need help with any information relating to credit union? Search a topic or ask any question below

in All 

SEARCH

Quick Actions

 Manage Users







 Edit CU Policies

 Edit CU BCP

 Manage Assignments





What would you like to view today?



 My 360 View Customize your experience.	 Compliance Information (InfoSight resources, policies, account insurance estimator)	 Model Content Comprehensive suite of content templates	 Published Documents Credit Union's custom content prepared for review.	 My Assignments 1 In Progress 1 Overdue	 APFCU Documents Files and resources uploaded by the credit union
---	--	--	---	---	---

News & Announcements

See All 

 Sep 24, 2024 What Is a Shared Branch Credit Union?	 Sep 24, 2024 Digital Federal Credit Union debuts self-service	 Sep 24, 2024 Colorado Credit Union makes retention a top	 Sep 24, 2024 Municipal Credit Union brings wealth
--	--	--	---



Additional Fraud Resources



- Required audit packages (BSA, ACH, SAFE Act, and Website Compliance Reviews).
- Resource Subscription including Risk Assessments (BSA/OFAC, ACH, Remote Worker, Social Media, Cybersecurity, and more).
- Internal audit services/outsourcing to protect against fraud and ensure safe and sound internal operations.
- Full-service customizable compliance management options for all asset sizes and needs.



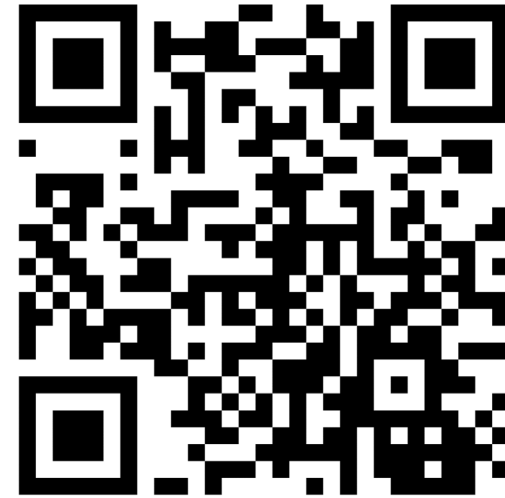
- Comprehensive complaint management tool.
- Self-driven compliance management system.



- Vendor management and regulatory due diligence with a dedicated analyst.
- Collection of due diligence documentation for all critical vendors annually.

Want more Information?

- **Reach out to your League/Association! They have strong partnerships offering many different tools and resources that can assist with Fraud!**
- I know this is a Fraud Symposium and we are using a QR code that has recently become a fraud mechanism... it's legit, but if you want to learn more you can always email us at: info@leagueinfosight.com!
- **Your League/Association Website!**
- <https://www.leagueinfosight.com/>
- <https://www.curiskintelligence.com/>
- <https://cuvvm.org/>



Thank

You