FIPCO FOCUS
COMPLIANT. CONSISTENT. CONFIDENT.
FEBRUARY 2018

2018 Deposit Compliance & Software Forum Expands to Two Locations

We are pleased to announce the host cities for the 2018 FIPCO Compliance and Software Forum – Deposit, and invite you to join us for our most important deposits event of the year. Geared towards the software user, these meetings will be held on May 15th at the Holiday Inn Madison at the American Center, and May 17th at the Grand Lodge Waterpark Resort, Rothschild.

"Our goal is to reach as many of our customers as possible," said FIPCO President, Pam Kelly. "By expanding this year's forum to two locations, and hosting at such fantastic venues, I'm confident our deposit software users will appreciate, and be able to capitalize upon the additional opportunities to participate in this year's event."

FIPCO COMPLIANT. CONSISTENT. CONFIDENT.
Compliance & Software Forum
DEPOSIT

May 15 · Holiday Inn Madison at the American Center · Madison
May 17 · Grand Lodge Waterpark Resort · Rothschild

With continued changes in compliance demands—like the upcoming BSA Beneficial Owner requirement, and Reg. CC Funds Availability, the timing of the conference is optimal for today's *Compliance Concierge*™ Deposit users. In addition to providing the skills and confidence needed to stay ahead of the compliance curve, the instruction you'll receive will help maximize the capabilities of your deposit software.

Whether you're new to FIPCO's *Compliance Concierge*™ Deposit software suite, or you've used it since its inception, this event offers the perfect opportunity to enhance your knowledge of this powerful software solution. Beginners will learn the fundamentals for expertly leveraging the software to increase efficiency and accuracy, and accomplished users can fine-tune their skills by learning about advanced system capabilities and upcoming system enhancements. As the conference draws near, we'll continue to keep you informed about complete session details and registration information. Be sure to watch your email inbox and the FIPCO website. We look forward to seeing you in May!

Updated Account Titling Handbook Now Available

We are pleased to announce the release of the WBA Account Titling Handbook – Revised 2017 Edition. If you've got questions about properly titling deposit accounts, this is a must-have resource! Available through FIPCO, this comprehensive handbook provides the most up-to-date, accurate, and authoritative information for your institution with guidance for opening accounts from basic to some of the most unique.

Thoroughly updated by WBA Legal Assistant Director, **Scott Birrenkott** and FIPCO Business Analyst – Deposits, Nancy Hamele, the handbook's usefulness cannot be understated. "The revised edition further modernizes this valuable information repository to assist financial institutions with adopting uniform procedures for titling and documenting new deposit accounts," Hamele said. "It really is an indispensable tool for anyone who works in the deposits field—and it's a trusted resource that I rely upon as well."

Not only does the handbook address common types of deposit accounts, it covers uncommon accounts such as Joint "and" accounts, Funeral, Lawyer, and Real Estate Trust accounts, as well as Benefit and Campaign accounts, and titling and documenting Municipal accounts.

Additional topics covered include Designation of Agent and POD Beneficiary, TINs and TIN matching, and the new Customer Due Diligence (CDD) rule requiring financial institutions to identify and verify beneficial owners of legal entity customers effective May 11, 2018.

"What's truly exciting," Hamele stated, "is that the new edition now includes form samples generated from *Compliance Concierge*™ – Deposit, providing our customers with precise information with meticulous attention to detail."

Complete details, including pricing discounts for Wisconsin Bankers Association (WBA) member institutions, can be found on the FIPCO website. Take advantage of this resource by placing your order today! Questions may be directed to the FIPCO Customer Service Department at (800) 722-3498, ext. 274.

» *Some of the many topics covered in the newly-revised Account Titling Handbook:*

- Titling of Personal, Business and Fiduciary Accounts
- Titling and Documentation of Municipal Accounts
- Designation of Agent (POA), and POD Beneficiary
- Taxpayer Identification Numbers (TINs)
- Customer Identification Program (CIP)
- Customer Due Diligence Rule (CDD) Beneficial Owner
- Special Rules for Certificates of Deposit
- Nontransferable Accounts
- Retitling Accounts

FIPCO FOCUS
COMPLIANT. CONSISTENT. CONFIDENT.
FEBRUARY 2018

See for Yourself How Managed IT Services Can Benefit Your Institution

Complimentary tour and informational event scheduled for March 6th.

In an industry that faces continued changes in technology, developments in Managed IT Services such as cloud computing can offer greater benefits and opportunities for today's financial institutions. We feel technology should work *for you*, which is why we recently partnered with UFS Data Center to offer *Compliance Concierge*™ Managed IT Services. Consider the following benefits:

- **Efficiency** – IT infrastructure updates and maintenance are eliminated, as all resources are maintained by UFS. Servers are off-premise, secure and out of sight, and UFS maintains the systems leaving you free to focus on the things that matter.
- **Security** – At UFS, multiple layers of security protect computer systems as well as all critical infrastructures supporting the facility. UFS' site security is managed, maintained and certified in SSAE-16 audits performed annually, which confirm they strictly adhere to the controls and processes consistently throughout the data center.
- **Savings** – Potential savings of $300 per month* on your IT costs.

We invite you to see for yourself how Managed IT Services through UFS can benefit your organization during our upcoming **FIPCO Hosted Environment Due Diligence Review** scheduled for **Tuesday, March 6th** from 10:30am – 1:30pm at the UFS Data Center in Grafton, WI. This enlightening event will include an introduction to FIPCO's Managed IT Services, UFS facility tour, as well as cyber security, regulatory, and operational performance discussions.

Todd Cearfoss, IT Manager for Bay Bank, Green Bay, attended the premiere Hosted Environment Due Diligence Review held in January, and recently stated, "I really think it's a good pairing for FIPCO, and this event at UFS really showcased that. It really puts the end user at ease with choosing this partnership."

Also among the January participants was **Stephanie Spencer**, AVP Operations and Information Security Officer for **The International Bank of Amherst**. "I was impressed with the facility and the security that is there," she said. "When the time comes for us to have our server hosted, we know it will be in good hands."

(continued)

Recent *Compliance Concierge*™ Update Supports MLA Interpretive Rule

Compliance remains our top priority.

In our organization's continued efforts to keep you ahead of the compliance curve, the FIPCO Software Development Team recently released an update to *Compliance Concierge*™ with modifications to several loan screens to comply with the Department of Defense (DoD) amendments to the Military Lending Act (MLA) Interpretive Rule. Here's what you need to know:

What's changed?

FIPCO has modified the **Loan Information Screen** (non-Real Estate) and the **Closing Information Screen** (Real Estate) "loan exemption" checkbox language that appears if a borrower is covered under the Military Lending Act (MLA). Users who have indicated there is a Covered Borrower(s) under the MLA are thereafter instructed to indicate (check the box) if the loan is exempt from the MLA. If the Loan is exempt from the MLA, the user will not receive MLA disclosures.

Why were the changes necessary?

The modifications were made to support an MLA Interpretive Rule issued by the Department of Defense on December 14, 2017. Under the Interpretive Rule, credit extended for the purpose of purchasing a motor vehicle or personal property, which also secures the credit, loses its exemption under the MLA where the creditor, as part of the transaction, also finances a credit-related product or service, such as credit insurance or GAP, or provides cash-out financing as part of the transaction. Other exemptions to the MLA, such as loans secured by a 1-4 unit dwelling (whether or not attached to real property), remain the same and can be found at 32 C.F.R. 232.3(f)(2).

Where can I find more information?

Lenders should familiarize themselves with these exemptions by reading the DoD's MLA Interpretive Rule and by reviewing FIPCO's full software release notes. You must be a registered user to access the release notes. Need a log-in? Click here to submit your request. Questions regarding MLA functionality in *Compliance Concierge*™ may be directed to the FIPCO Software Support Department at (800) 722-3498.

Managed IT Services Event *(continued)*

We look forward to seeing you on March 6th. Lunch will be provided during this event, and **there is no cost to participate**, but advance registration is required to attend. Contact us today at (800) 722-3498, ext. 258 to reserve your spot.

*Cost savings may vary based on your IT costs.

FIPCO FOCUS
COMPLIANT. CONSISTENT. CONFIDENT.
FEBRUARY 2018

Is a Continuous Diagnostics and Mitigation Program Right for Your Institution?

There are many practical considerations that can be leveraged when implementing a National Institute of Standards and Technology (NIST) Continuous Diagnostics and Mitigation (CDM) Program. In this article, we'll identify a few practices to support your implementation of a CDM Program, with the hope that the information provided can be used to assist an organization with aligning CDM into the current information security program, or meet requirements of another cybersecurity management structure such as the NIST Cybersecurity Framework (CSF).

CDM is a dynamic approach to fortifying the cybersecurity of networks and systems. By using CDM, organizations can arm themselves with the additional security capabilities and tools needed to establish a proactive and ongoing prioritization of risks based on potential impacts to valuable assets, and the likelihood of a risk occurring. By having a CDM program in place, security personnel will be better prepared to mitigate and prioritize problems with the highest impact, and those most likely to occur.

The NIST CDM Program consists of three phases, and is designed to cover continuous diagnostic security capabilities:

1. **Endpoint Integrity** – focuses on control areas related to the management of hardware and software assets, configuration management, and vulnerability management. These can also be looked at as the basic foundations of any robust information (cyber) security program built to protect systems and data, by addressing hardware and software, as well as configuration settings and vulnerability management.

(continued)

2. **Least Privilege and Infrastructure Integrity** – brings together some of the "trust" related controls of the phrase "Trust but Verify" by considering the requirements of access and authentication; identifying users and privileges for who can do what, and the idea that these need to be managed on an independent, continuous, and proactive basis. This phase also introduces the first parts of the verify process by considering "Behavior Management" as it relates to security.
3. **Boundary Protection and Event Management** – provides for the management of the entire Security Lifecycle, and furthers the idea of "verify" with controls related to monitoring. This phase consists of the security areas including planning for, and responding to events, generic audit/monitoring, documenting requirements and policies, as well as risk management and boundary protection.

When implementing continuous monitoring, organizations may need to increase the amount of data captured, automate collection of events across numerous systems – essentially centralizing the collection, and in the end, hopefully make organizations better-equipped to prioritize risk alerts. And once the CDM Program is implemented across the organization, there will be a comprehensive, and continuous security infrastructure in place.

There is much to consider when determining whether a CDM Program is right for your institution, and this article merely scratches the surface. This article was a consolidation from a soon to be published chapter in the International Guide to Cybersecurity, 2nd edition published by the American Bar Association. For further information, as well as links to additional helpful resources, please contact FIPCO Director – InfoSec and Audit Services, Ken Shaurette at (800) 722-3498, ext. 251.

IT Peer-Group Event

We're continuing our series of Threat Intelligence Briefings throughout 2018 and invite you to join us February 15 in Stevens Point. Network, discuss current IT issues with your peers, and receive 2 hours of continuing education credit for information security training when you attend. Space is limited and will fill quickly so be sure to register today!

February Software Training

(All events are *Compliance Concierge*™ training courses.)

Feb. 5-8, 8:30 – 4pm:	Loan and Mortgage 4-day Training
Feb. 13, 9 – 11am:	Commercial Webinar
Feb. 13, 1:30 – 3:30pm:	Ag Loans Webinar
Feb. 15, 1:30 – 4:30pm:	Deposit Accounts Webinar
Feb. 20, 9 – 11am:	Real Estate Purchase Webinar
Feb. 20, 1:30 – 3:30pm:	Real Estate Refinance Webinar
Feb. 22, 1:30 – 3:30pm:	Basic Consumer Loans Webinar

Visit the FIPCO website, or contact the FIPCO Training Department at (800) 722-3498.

4721 South Biltmore Lane | Madison, WI 53718
P: 800.722.3498 | F: 608.661.9382 | fipcosales@fipco.com
www.fipco.com