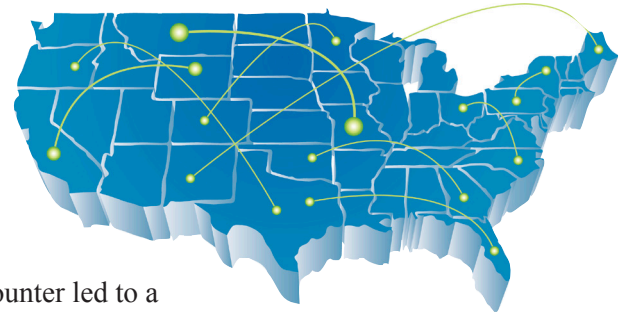


Real Life Examples of Member Value Peer-to-Peer Networking

Learning from credit union peers around the country has always been a fabric of our cooperative. Many members who attend Alloya events, have developed strong peer networks that broaden their exposure to industry issues. The strength of credit union peer-to-peer networks is that you are among professionals that face similar issues. This fuels the ideal environment for sharing and growing.

During last year's Credit Union Executive Leadership Symposium, in addition to the educational sessions, the effectiveness of peer-to-peer networking was a major highlight. Rob Marlatt, one of Alloya's Senior Business Consultants, was aware that a member attending the symposium had independently engaged in some loan participations with other credit unions in the past – and he knew that they were still in the market to sell loans. Rob introduced this member to Bill Paton, Alloya's Assistant Vice President, Lending & Participations. This encounter led to a discussion with another credit union at the symposium that happened to be looking to buy loans. With Bill as the intermediary, the two credit union executives agreed to work with each other through Alloya's Loan Participations program.



“Working with Alloya's Loan Participations program was ideal and well worth the 25 basis points for many reasons,” said the selling credit union executive. “It has more weight when a third party is involved. Alloya handled all the questions from us (the seller) and the buyer – and the transaction stayed within the credit union network.”

“The networking that occurs at Alloya's events is electric,” said Bill Paton. “Members have swapped stories, shared laughs and made strategic plans that would not have occurred without the opportunity to meet colleagues in person. As credit unions, we all need each other – and Alloya is always thrilled to facilitate the conversation.”



September 6-8, 2017 ■ Chicago, IL

What credit unions are saying...

“The symposium provides me with a lot of focused credit union education. Plus, I get to hear from a variety of presenters that help me think in different ways.”

“It's been a wonderful experience to be around so many credit union people from all over the country.”

“There are so many reasons to attend: the content and presenters, networking, no pushy sales ploys, the setting – and the biggest reason for me – I gain CPE credits.”

Don't miss out! Learn more at
www.alloyacorp.org/symposium2017

BALANCE SHEET SOLUTIONS

— an alloya company —

Connection Webinars Save-the-Dates

Reviewing Your ALCO Program

July 13, 2017, 2:00 pm ET

Enhancing Your Investment Decisions

August 10, 2017, 2:00 pm ET

Details and registration will be made available at:
www.balancesheetsolutions.org/learn_webinars

Protecting Data and the Systems You Utilize

The explosion of online banking and mobile computing has introduced many opportunities for bad guys to commit fraud by stealing credentials or taking over accounts.

So, what is your corporate doing to protect your data? Three examples of how Alloya is safeguarding your information:

1. Protecting Our Online Transaction Portal – Premier View

Nothing is ever 100% secure, but we put a lot of time and effort towards making Premier View come close to that mark. For any authorized user to access Premier View, they must login using an authentication process that includes:

- User enrollment
- Machine registration
- Identification and password entry
- One-time password token response

Plus, Trusteer Rapport – a leading anti-malware program that provides additional protection to combat the ever-changing information security threat landscape and protects the integrity of Premier View transactions.

2. Security Training

For Alloya Staff: Routine training is provided to ensure that they are educated on potential information security threats such as phishing, malware, identity theft and account takeover as well as any new threats that impact security, such as the recent “WannaCry” ransomware attack. WannaCry was a malicious software program that encrypted the data on targeted computers, thus making systems unavailable until a ransom is paid.

For Alloya Members: In addition to posting security alerts on Premier View and the available recorded trainings, we provide live educational webinars and are available to speak at chapter events. This education really helps us to connect with members and better understand the concerns they have about information security and fraud.

3. Compliance Reviews

For example, all foreign items are reviewed by Alloya and Western Union. As a high-risk payment type, foreign items have a greater risk of involving an entity or jurisdiction, which may violate a U.S. sanction. To comply with Office of Foreign Assets Control (OFAC) compliance regulations and avoid potential penalties, payment details inputted by your credit union staff into the Western Union Business Solutions Global Pay system are screened against OFAC sanctions listings. This allows your credit union to be made aware of any potential OFAC matches prior to your staff mailing the foreign item(s).

For any general questions about how to stay safe online, please contact your Senior Business Consultant.



Dean’s Security Tips

Helpful tips to keep your systems secure with Dean Choudhri, Assistant Vice President, Information Security

- ❶ Members need to continue to be aware that malicious software programs are often installed on computers by clicking on links or attachments in phishing emails or by visiting infected websites.
- ❷ Do not give your users authority to install software or any other programs on their computers. A separate account, which is not used for normal day-to-day activity, should be used to install software and programs on computers.
- ❸ Ensure that security updates and patches are installed regularly. Critical patches should be installed within two weeks of being released by the vendor.
- ❹ Only use software (Windows, Adobe, etc.) that is supported by the vendor. Vulnerabilities with out-of-date software are often exploited by hackers.