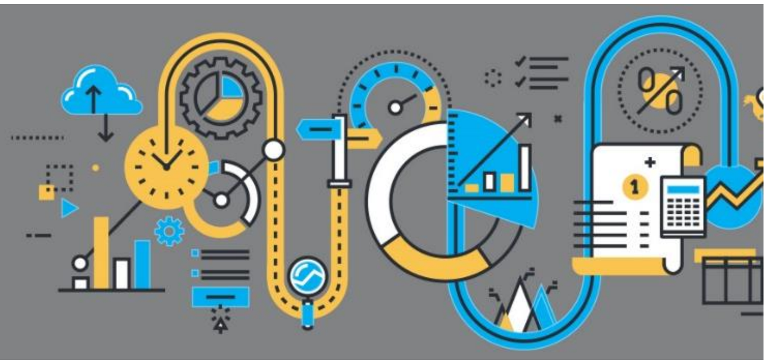
CU*ANSWERS
A Credit Union Service Organization

CEO Strategies Week 2016

Scribe Notes



Group 1

Scribe - Julie Gessner

Name	Credit Union
Barbara Harper	Cincinnati Ohio Police Federal Credit Union
Kim Kniola	First Trust Credit Union
Russ Dalke	Northern Colorado Credit Union
Todd Powell	Spokane Firefighters Credit Union
Barbara Bean	Cal Poly Federal Credit Union

Group 2

Scribe - Liz Winninger

Name	Credit Union
William Burke	Day Air Credit Union
Charles Papenfus	Inland Valley Credit Union
Randy Gailey	Horizon Credit Union (Utah)
Karen Browne	TBA Credit Union
Janet Borer	Members First Credit Union

Group 3

Scribe - Esteban Camargo

Name	Credit Union
Leo Vaulin	CU*South
Steve Kelly	Metrum Community CU
Patrick Post	Mountain River CU
Scott Collins	Xtend
Kim Hall	Tri-Cities CU
Todd Powell	Spokane Firefighters CU
Russ Dalke	Northern Colorado CU

Group 4

Scribe - Laura Zazakis

Name	Credit Union
Scott McFarland	Honor CU
Greg Smith	CU*NW
Tom Gryp	Notre Dame Federal CU
Adam Johnson	Safe Harbor CU
Carma Peters	Michigan Legacy CU
Karen Browne	TBA CU

Group 5

Scribe - Barbara Cooper

Name	Credit Union
Jeff Jorgensen	Sioux Empire
Michael Abraham	First Financial
Vin Cerasuolo	Century Heritage
Lindsey Merritt	Jordan CU
Kevin Posey	Thinkwise CU

Group 6

Scribe - Keegan Daniel

Name	Credit Union
Linda Bodie	Element
Dean Wilson	Focus
Don Mills	Alpena Alcona
Kevin Ralofsky	Verve
Dennis Degenhardt	Glacier Hills
Jerry Wise	Greensboro

Group 7

Scribe - Marsha Sapino

Name	Credit Union
Christy Leslie	Bridge CU
Barb Mills	Calcite CU
Mark Richter	First United
Kim Bourdo	Service 1 FCU
Charles Papenfus	Inland Valley CU
Barbara Bean	Cal Poly FCU

Group 8

Scribe - Jim Vilker

Name	Credit Union
Barb Page	Kent County
Corrine Coyie	Advantage
Vickie Schmitzer	Frankenmuth
Matt Jennings	Quest
Janelle Franke	River
Randy Gailey	Horizons
Steven Janssen	Brewery
Andy Fogle	Des Moines Police Officers

Group 9

Scribe - Annalyn Hawkes

Name	Credit Union
Mike Brandt	Evergreen CU
Steve Janssen	Brewery CU
Jerry Wise	Greensboro Municipal CU
Jennifer Oliver	South Bay CU
Kris Lewis	Allegan CU
Andy Fogle	Des Moines Police Officers

Group Notes

The following notes are included exactly as taken by table scribes. Scribes were instructed to jot down everything that was discussed at the table, with the idea that reading the notes would be a little bit like eavesdropping on the conversations.

Fraud and Denial of Service

As peers, what are you thinking about new fraud services and future systems that will deny transactions for you?

- When do you want a computer to **deny a transaction** or **delay a member's request**? What do you think about your procedures for interpreting that a member is really the member?
- What is the difference between cross-channel fraud analysis and direct channel analysis? Can we design a better mousetrap the next time around?
- Can you afford the duplication of expenses for channel specific fraud protection investments? How are you planning to improve your programs in 2017 and beyond?

Group 1

- Not just the card – how can we give members control of the account? There are a lot of facets that need to be considered. Let the planning begin. We have to consider this as something we have to have.
- Using data for behavioral economics. Down to the member. This would slow down friendly fraud.
- Really consider the amount of fraud you are willing to write off.
- Consider timing for debit card re-issues.

- Controls are coming. Consider the lowest common denominator – what happens when the member is shut off and doesn't know how to turn it back on?
- At some point regulators are going to say you have to have debit card controls in place
- Cross-Channel Fraud vs. Direct Channel is difficult to define
- Building a better mousetrap with a signal source denial point is far better than trying to control it from different relationships. Explaining to members would also be better.
- Educating staff on how they will educate and communicate to members
- PIB – encouraged with business members. Especially those with agents. Using PIB restricts access. Doing this can become complicated for members.
- The crooks are getting smarter. We don't have time to management this. We need a process that is simpler and secure. If we are just a little better than everyone else the fraudsters start looking somewhere else.
- Concentration of areas that are your biggest headaches. Shared Branching is becoming a bigger threat.
- Can we afford duplicate controls: By comparing our options with the things people want we can control our expense and remain competitive. Card Nav. Is one of those things. The cost is absorbed but this is something we can do to control the fraud and give member control.
- We can't charge members for anything. People do not want to pay for anything.
- In today's society members are getting younger. They don't pay attention to other traditional forms of communication. We can educate them using other delivery channels. If you want members to know text them.
- We will always look at improving. It would be amazing if there was a one-time solution that covered it all. I would like CUA to come up with a solution to turn on and off the overdraft and lines of credit controlled by the member.

Group 2

- These computer model algorithms are our best friend and worst enemy. Though they secure our members from fraud, computer models are as good as the data in them. Also, securing our members takes some time from the first point of purchase. How does the clerk not flag the purchase? Our algorithms help, but we can't rely on the retailers to help members as well (someone buying $15,000 of Target gift cards in under 10 min.).
- The future of fraud prevention is exciting and we hope to get our members educated so they will use the technologies coming (shut off your card if you lose it, limit transaction amounts, etc.). We are telling our members how to turn on the transaction notification, but not all of the other features. We also want to make sure our members understand the importance of preventing fraud – because to them, they get their money back, we want to get them more invested in why they should help prevent fraud.
- **If they are unwilling to use the software, we will limit their transactions/transactional amounts.**
- We want to limit the card spending.
- We are preventing transactions at Wal-Marts for anything between $40-$50. We deny them. We get hundreds of fraud transactions on those limits each day. Another cu noted that a lot of fraud is coming in through gas stations right around the $99 amount.
- An option in the coming technologies that is also exciting for cu's in regards to prevention is the ability to limit transactions that are a specific distance away from your phone.
- One great feature was being able to quickly search in Gold who shops as a specific vendor location, then contact those members and shut those cards down.

- Peer to peer and lending club vs. Facebook loans should we be thinking out of the box on how to make loans**.**

Group 3

- Fraud has gone up in recent years; so fraud prevention services are a worthwhile investment even if they can be frustrating to both us and the members. There's no doubt systems need to be improved, but we can't ignore the rising numbers.
- As cooperatives, we need to figure out ways to bring fraud prevention services inside. Vendors like Falcon and On-Dot don't like sharing their data, so you have all these services operating on islands. Bringing it within the cooperative provides an opportunity for smarter (and cheaper) fraud prevention services.
- Merchants have started using Pinless PIN more aggressively, and it causes complications on our end.
- We have to do more to protect member information because retailers don't care.
- Would like to see on the DP side a notification system that allows members to stop fraud as they see it start, more than a denial of request service.

Group 4

- **Scott** - Charge a cyber security fee if members don't participate.
- Different checking levels – reward for logging in, changing password, etc. Need to be active
- Cyber secure checking – member pays if they don't use it.
- **Carma** – Believe artificial intelligence over staff. Biggest fraud at teller line. Created a hot-line. Staff remote access 24 hrs a day, so if card is denied, then member can call. Business for Xtend?
- Zip whip – call center uses for texting members, and members can text CU. Member feedback is great. Per Scott, can't do anything secure. Text connected to an email address. Almost like a chat window for the user.
- Create a response environment for the members. Software within secure network, but members phone is not secure, so caution about secure data.
- **Tom** – As long as the computer makes the right decision…then all for it. Are we willing to expose our members to the frustration, while we learn how to be better in the future? Notre Dame CU uses MOBI money for debit and credit cards. User controls and can turn card on and off. CU pays for the fee.
- The CU has over 30,000 debit/credit cards, need to determine how many are high risk. Spend money marketing to high risk.
- Went with on-dot and personalized. The quicker we can come to market the better
- **Greg** – If you want to take more risk, multi-layer authentication. Wide range of member tolerance to risk. Driving home to member no perfect science, ask member to provide
- Great idea - Text message on your transaction. Notification to member for each transaction. To know that every transaction comes to cell phone is piece of mind. Should we build a collaborative solution?
- **If we build internally we can pattern across entire network to have a wider view**. More information to make reference and make a decision. Do something that no one has done. We have an opportunity to build in at core level.
- Build SMS texting into core. Let member set level of visibility.

Group 5

- Table: Wants to give members the ability to turn off their card and turn it real-time.

- Agrees that members rarely assume the cost of a fraud/breach, so steps to prevent fraud is not taken as seriously as it should.
- Wants CU*A to perform fraud protection – it only makes sense.
- Vantiv's Mobi-money makes sense for now.
- Most of the credit unions at the table budget for fraud expense.
- Jeff: We need to better manage our duplication of fraud protection over all channels to reduce duplicity.
- Michael: Budgets for fraud – taking historical values and adding a percent increase each year. Buying insurance costs more with high deductibles than actual loss. In addition, claims result in higher premiums.
- Member Check fraud costs the credit union as the disputed transaction cannot be processed in time to recoup the fraud amount.
- Summary: Carma Peters – Michigan Legacy, Offered a collaborative approach for a business with more than one CU for protection for all channels, with one phone number (XTEND?) to handle the protection support, and member services such as traveling to foreign countries, etc. (Randy called on Dave Wordhouse, Brian Maurer to work with Carma for how this business would work.) Randy is concerned (based on prior experience) that CU*A builds this CUSO, he's worried if the CU's will turn it on.
- Mark – First United: Making sure the fraud protection experience for the members is improved with better communication. Use alerts for plastic transactions to notify the member. The key is to manage the member experience for positive emotions.
- CU*A sells Paywatch, (offered by PayVeris for Bill Payments) at .02 cents per transaction. You do need to work suspicious transactions submitted to the credit union. We have 6 or so clients using this product.
- Another question from Randy – Does CU*A know the key person at the credit union to call who makes the decision to turn off It's Me 247, bill pay etc. Currently CU*A does not have a formal form to know who these people are. We start at the CEO and work our way down. Should we move down this road?

Group 6

- How do we get beyond geofencing (DW)?
    - And how does this have an impact on our retail experience?
- I prefer a complicated approach (LB)
    - I want to be notified of charges via text
    - Dual authentication, etc.
    - Mitigate as much as possible
- We have become experts (not by our own choice…) at budgeting for Debit/Credit card fraud (DM)
- We need to review the card control tools that are being brought to the marketplace. (DD)
- Members get more upset about waiting for a card rather than hearing about a compromise (KR)
- Until the member cares, our efforts may be futile (DW)
    - How do we create an informed consumer/member?
- How are we supposed to 'Burn It Down' when topics are depressing?
- If we deny service, will members just use another card in their wallet (DW)?
- Fraudsters have focused primarily on debit cards. Will there be an expansion fo fraud in the credit card arena?
- Should we manage shared branching controls in a similar fashion (LB)?

Group 7

- First United
  - Reminds me of how we started using Falcon and preparing our staff's reactions
  - Agree that consumers are becoming more accepting of denials
  - Out of wallet questions. Don't say 'no'. Just say 'not now'.
- Calcite
  - Members are becoming a little more understanding of denials
  - We don't really have procedures in place of how to respond to member contact regarding denial
  - If we have the tools in the core, we would probably turn it on
  - What is abnormal?
  - Love the idea of building the software for notifications but what is it? How much are we willing to pay?
  - One solution would be so much better than multiple ones and still have a good experience
  - We don't think we will be turning MOP on. We are not there yet.
- Bridge
  - If we don't come up with a solution we feel we will be made to do it eventually in regulations
  - Improve Abnormal Activity monitoring real time
  - Plastics system has pretty much figured out the logic.
- Service 1
  - Hard to compete with the notification services the bigger organizations have? Get a text saying you are doing a transaction and you reply NO and within a few minutes, you are getting a phone call.
- Conversation went off topic after they felt comfortable with the current subject
- The opening of accounts online and how they are verifying the identity of individuals.
- Then discussed how they are retaining their documents (edoc).
- First United is virtual strong box.
- Discussed encrypted email. Calcite is using ZIX and the members don't mind it at all.

Group 8

- Deny and delay should be at the member's discretion. Credit Unions lock it down and the member can open it back happen. Vickie wants the transaction verification.
- Credit unions are using other vendors such as credit and debit card. Janelle had moby money and have invested to let members manage the fraud. Another had ondot and another had secure lock. Vendor are providing it
- Do it all, not just bits and pieces
- Discussion was if CU*Answers did it they would not have to pay so many vendors to buy pieces
- Discussed that CU*Answers is tracking what the member does through all channels rather than one channel
- Cards, It's Me 247, Bill Pay, and ACH, shared branching channels consider flagging teller that this is not normal activity
- Have AuditLink monitor changes in e-mail addresses
- Matt said that reducing the number of vendors would lead to spending only on one for fraud detection

- Matt wants to give the member the tool but make the member ultimately responsible for setting it up and pulling the levers
- Putting some responsibility on the members was discussed at length
- Some have shut down states and other stores in an entire state
- Vickie thinks that they should be budgeting for fraud protection instead of budgeting for losses

Group 9

Debit Card Fraud Programs

- We've been saying no to our members for quite a while. Our debit card processor's fraud management is default and some of it's after the fact. We do get those angry calls from members. Usually when we explain why they will understand. (Mike)
- I've tested my card fraud security recently. I usually get away with it. Only one time recently I was in Texas and I was able to buy one thing, then next purchase was denied. (Kris)

Apps for Member Management of their own Debit Card

- Shazam
- Vantiv
- Existing issues with Shazam compatibility with CU*A when CU*A goes offline, limits shoot up. (Mike)
- I see (the app) as a revenue stream. (Kris)

Great but how do you get members to use it?

- CEOs understand all the reasons and factors of these, but do our members understand this? (Steve)
- But is it more that they don't care rather than not understanding? (Mike)
- Members don't want to have to be in control of that. They have the mentality that it's not their responsibility. Part of it's because why would they even need to bother. I think you would want to incentivize them instead of charge them (Jennifer)
- How would you track or know whether or not they're actively using (the app)?
    - Education is going to be so important in the account-processing process to get people to use (the app) (Kris)
- Truly 25% of people will just say yes if you just put (the app) in front of them. They may not need it, or understand it, but they will say yes (Mike)

Aggregating data storage & analysis

Automated Transactions Denied – Do we tell our members no without checking with them first?

- I've had members actually thank me. Once you've explained the process and why, members say "ohhh, ok" (Jerry)
    - I think our members would be ready for us to say no based on a computer decision. (Steve)
    - If we have better, stronger data, we would say no less often. Less false-positives. (Jennifer)
- So the aggregation of this data – do our data processors do that today? They don't! (Jerry)
- I want to see "cross-pollination" by CU*Answers overlooking the data across all CUs to look for trends and then automatically make a new rule. I don't even want to know about it until they've done it. (Mike)

- And when system-wide attacks happen you want CU*Answers to be able to act quickly (Jennifer)
- CU*Answers can come in and be the central place that reviews/sets rules for cross-channel data (Bill Pay, P2P, Debit, Credit, etc). (Jerry)

What about those of us who use other not-so-compatible vendors?

- That has to be an individual CU decision and that can really drive decisions into more and more connected/aggregated solutions.

Are we even aware of what can happen? What the possibilities are? (Jerry)

- It's an analyst. Someone needs to be looking at behavior. It's not proprietary, it's normal computer science. Either we have all these systems externally, or we aggregate it (Jennifer)
- I'd rather spend (a large amount of money) all to CU*Answers for all this together. (Kris)
    - Artificial intelligence is what it is. It's all there, it's just a matter of making the investment (Jennifer)

Chip Cards

- They don't do anything – 75% to 80% of fraud is happening online. I tell this to my members to explain why we haven't switched over to Chip Cards. They generally understand. (Mike)
- (Chip cards) have been around in Europe for many years so in a way it's just as if we're adapting old technology by this point (Jerry)

Reaction vs Prevention

- Cybersecurity is trying to protect the credit union. Fraud is trying to protect the member data (Jerry)
    - Most important to worry about is how to react to it, rather than so much of questioning how do I prevent it. (Kris, Steve, Jennifer)
- That way of thinking works at a smaller sized credit union, but when you get to larger size how does that change? (Mike) Scaling and data analysis allow the same effect for larger CUs (Jennifer & Kris)