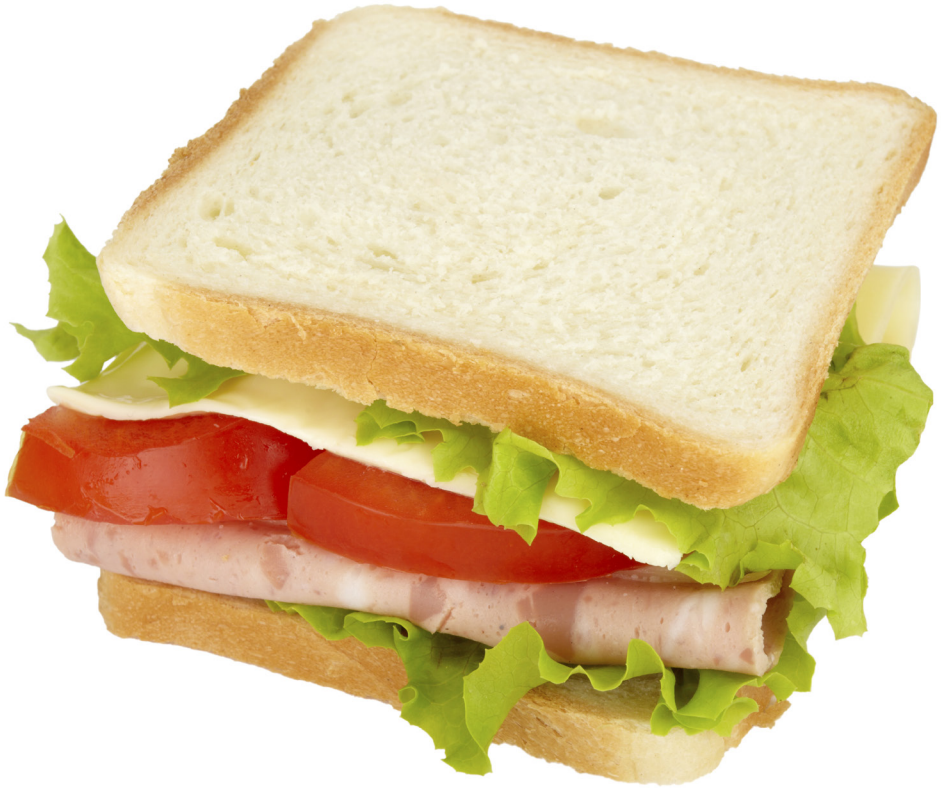
Issue 8 | June 2014

Network Compliance Teacher

Compliance News and Tips from Credit Union Compliance Officers
sponsored by CU*Answers AuditLink

In this Issue...



Editor's Corner

This quarterly edition is a bit different than those in the past. It remains our mantra to have our credit union peers educate each other through articles posted in the NCT but this edition has taken a bit of a different tack. Over the course of the last few months we have requested that industry experts also supply material and as you can see we hit the jack pot.

For those of you familiar with NAFCU, you will immediately recognize Steve Van Beek and understand how lucky Michigan is with his return. Steve, formerly one of the top compliance professionals at NAFCU, moved back to his home state and is now working as an attorney at Howard and Howard. His article on common credit card act violations resonates with me as my belief is many of us have forgotten some of the topics he discusses. Enjoy this 8th edition and get ready for an upcoming call out for authors for our next publications.

Jim Vilker, NCCO
VP of Professional Services
CU*Answers

Get Involved with the Network Compliance Teacher!

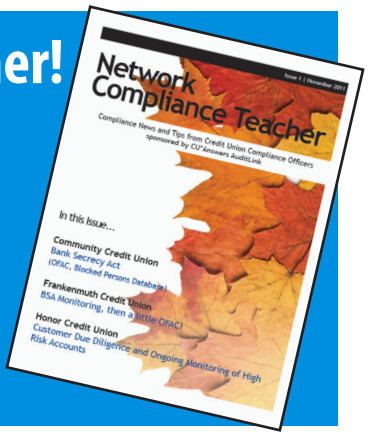
Have something to contribute?

Want to write an article for a future Network Compliance Teacher Issue?

Have a topic to suggest for a future issue?

We're looking for compliance officers like you to contribute!

Contact AuditLink at auditlink.cuanswers.com



The Network Compliance Teacher is a collaboration of compliance minded Credit Union Professionals like you from throughout the cuasterisk.com network.

The Network Compliance Teacher is published quarterly. Current and previous issues are available for download from the AuditLink website at http://auditlink.cuanswers.com.

AuditLink
CU*ANSWERS Management Services

6000 28th Street SE
Grand Rapids, MI 49525
(800) 327-3478
auditlink.cuanswers.com

Proud Member of the cuasterisk.com Network

5 Common Credit CARD Act Violations

Steven Van Beek
Attorney and Counselor
Howard and Howard

Auditor

It has been almost five years since the Credit CARD Act was passed by Congress and more than four years since the compliance dates set by the Federal Reserve Board (many compliance professionals may still be haunted by the date February 22, 2010). While it would seem like credit card compliance issues are in the rearview mirror, now is the perfect time for credit unions to review their procedures to ensure they remain compliant.

And, a lot has happened in the past four years - most notably the passage of the Dodd-Frank Act and the subsequent creation of the Consumer Financial Protection Bureau (CFPB). Now that the CFPB has met its Dodd-Frank mandates, its attorneys are freed-up to review other areas of concern – including credit cards.

Below are 5 Common Credit Card Violations that credit unions should be reviewing and, if necessary, correcting.

Increasing APR or Fees in First Year

One of the key components of the Credit CARD Act was the restrictions on when credit unions could increase a member's APR or a fee on a credit card account. Now, credit unions must utilize one of the exceptions in Regulation Z before taking an action that would be adverse to members. A common approach is using the 45-day advance notice exception – which allows credit unions to increase the APR (on future purchases) or a fee provided the credit union has properly notified members in advance of the increase.

However, this exception comes with one large compliance hurdle: it cannot be used during the first year a member's credit card account has been opened. Thus, credit unions that are implementing "across the board" APR or fee increases must be tracking and monitoring which members opened their credit card accounts in the prior twelve months and delay the increase on those accounts until the first year has ended.

Rate Reevaluations Every 6 Months

Related to the first common violation, the Credit CARD Act added an affirmative requirement to monitor – at least every six months – accounts where the credit union increased the APR. This requirement applies for both "across the board" and "individual" APR increases – such as when a particular member's credit score has dropped. In these situations, the credit union must review the rationale for the APR increase and, importantly, document its decision to not reduce (or only partial reduce) the APR on the account. Unfortunately, this rate reevaluation obligation only ends when the member's account is reduce to the original APR.

Additionally, credit unions that have acquired credit card portfolios via a merger step into the shoes of the original creditor and must review the APR increases conducted by the prior credit union.

Caps on Penalty Fees

In a unique move, Congress also gave the Federal Reserve Board (and, now, the CFPB) the ability to place caps on certain penalty fees. These include late payment fees, returned payment fees and over-the-limit fees. In these situations, credit unions are limited in the amount of the fee that can be charged. For the first violation in a six month period, credit unions have a "safe harbor" of compliance if their fee is $26.00 or less and for the second violation – of the same type – in the same six month period, credit unions can charge up to $37.00.

Beyond the initial caps, credit unions are prohibited from charging a fee that is larger the amount of the transaction. This "reasonable and proportional" requirement means a credit union cannot charge a $26.00 late fee if a member misses a $20.00 minimum payment on their credit card. In that situation, a credit union could not charge more than $20.00 for the late fee.

Increased Credit Limits

The Credit CARD Act created an ability to pay test that credit unions must consider prior to opening a credit card account or increasing a member's credit limit. Additionally, specific protections were put in place for members who were under the age of 21. In these situations, a member

continued on page 6

Are you Social Media Compliant?

Deb Schaffer, CCUFC
Business Development/Consultant
Chatter Yak!

Marketing and Compliance

For many credit unions, social media compliance is still a mystery. Does it exist or doesn't it? Social media compliance does exist. And because it exists, you must not only become familiar with it, you must incorporate it into your marketing plan. Chatter Yak! (a CUSO with whom CU*Answers recently partnered) encounters and trains credit unions daily who are still unaware that the "Guidelines for Social Media Compliance" document exists. The FFIEC (Federal Financial Institution Examination Council) produced an official 19-page document in December of 2013.

What you should know about the guidance:

- It is intended to help financial institutions understand and successfully manage the potential risks regarding the use of social media.
- It clarifies that existing consumer protection and compliance laws and regulations apply to activities conducted by financial institutions through social media as they would to activities conducted through other channels.
- It reminds institutions that they must properly address risks, including compliance, operational, third-party, and reputation risks, that arise in connection with social media activities, and it does not impose any new requirements on financial institutions.

In order to eliminate the mystery, or simplify this for your credit union, let's focus on Page 7 of the document. Here, the FFIEC states that you must have a risk management program in place. Components of your risk management program must include:

1. A risk management program that allows you to identify, measure, monitor, and control the risks related to social media
2. An employee-training program that incorporates your policies and procedures for official, work-related use of social media, and potentially for other uses of social media, including defining impermissible activities
3. Parameters for providing appropriate reporting to your board of directors or senior management that enable periodic evaluation of the effectiveness of your social media program and whether your program is achieving its stated objectives
4. Policies and procedures (either stand-alone or incorporated into other policies and procedures) regarding the use and monitoring of social media and compliance with all applicable consumer protection laws and regulations, and incorporation of guidance as appropriate; Further, policies and procedures should incorporate methodologies to address risks from online postings, edits, replies, and retention.
5. A governance structure with clear roles and responsibilities whereby the board of directors or senior management direct how using social media contributes to the strategic goals of the institution (for example, through increasing brand awareness, product advertising, or researching new customer bases) and establish controls and ongoing assessment of risk in social media activities
6. You are expected to take steps to ensure that advertising, account origination, and document retention are performed in compliance with applicable consumer protection and compliance laws and regulations (i.e. Regs DD, E, B, Z, etc.)

continued on page 3

What is FraudNet?

Angel McConer
EFT Support Specialist
CU*Answers SettleMINT

Back Office

FraudNet is a fraud prevention software that CU*Answers purchased in 2013 that detects potential fraudulent activity over Fiserv Bill Pay (formerly CheckFree). FraudNet connects a network of fraud professionals from multiple financial institutions. Such a network of participating professionals in credit unions, banks, and brokerage firms shares the data, allows a larger protection net. FraudNet uses Fiserv's payment-processing data across the entire network to detect fraud. By connecting the different entities with this common interface and detection tool, the system continues to grow and reduce the costs of fraudulent activity.

FraudNet is automatically working 24 hours a day, 7 days a week to detect suspicious activity. If the predetermined threshold is met, an alert is generated. Beginning the moment a subscriber schedules a payment, the data is transmitted in real time into Fiserv's mainframe. Since FraudNet interfaces with Fiserv's mainframe, the transaction is placed in a pending status prior to processing. The pending status is brief yet long enough to analyze the transaction, which will then process or trigger an alert. The transaction is matched against the different variables to determine if a threat is warranted.

In the event an alert is triggered, another part of the team comes into action. The specified credit union representatives will be provided an alert via AnswerBook. It is important to review the alert in a timely manner to help protect the subscribers. Be cautious of time since this is a time-sensitive matter. Once you have completed your investigation based on your internal fraud procedures, you will need to contact the CU*Answers SettleMINT EFT team by responding to the AnswerBook incident or calling us directly at 800-327-3478, ext. 309. When contacting the team, you will inform us to release or reject the payment. If fraud is detected, the team will need to know as much information as possible to assist in catching the perpetrator. You'll also need to identify the type of fraud such as an account takeover, ID theft, bank fraud, friendly fraud, or electronic payment kiting.

NCT

Social Media Compliance

continued from page 2

7. Procedures in place to address risks from occurrences such as members of the public posting confidential or sensitive information such as account numbers on the social media page or site you are using
8. Policies in place to monitor and address in a timely manner the fraudulent use of your credit union's brand, such as through phishing or spoofing attacks
9. Protocol regarding a security event, such as a data breach or account takeover, should include social media, as appropriate.

Has your social media manager been trained on effective use of social media for your credit union? Further, have they since trained your staff on acceptable work-related use of social media, clearly defining impermissible activities through your credit union's social media policy, and have your employees signed a social media policy acknowledgement form? If you cannot answer yes to both of these questions, start here. Then, continue building your risk management program with the remaining components.

With proper training, the mystery will be solved, and your credit union will mitigate risk and remain compliant… music to the ears of your board, management team, and examiners.

NCT

A Risk Assessment of the Proposed Rule on Risk Based Pricing

Jim Vilker, NCCO
VP Professional Services
CU*Answers

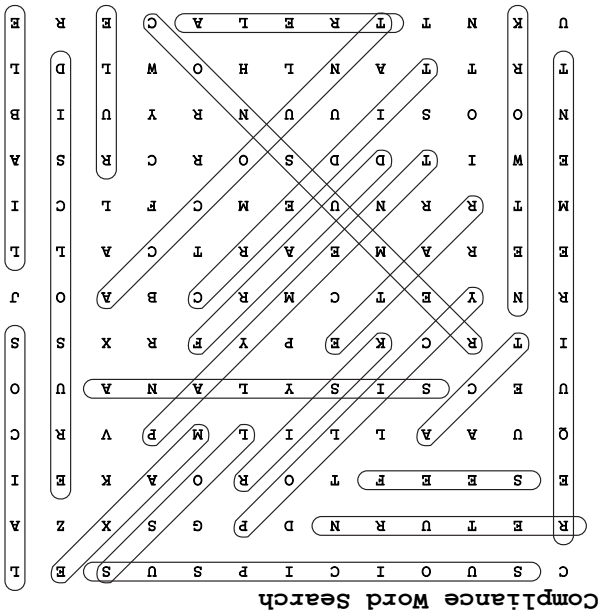
All Departments

Many CEOs, CFOs, and industry compliance professionals have weighed in on the nuances of the proposed regulation regarding Risk Based Capital (RBC). Despite the fact that unsecured loans carry less weight than real estate loans and that investments in CUSOs do not take into account the balance sheet of that organization, the new, high rate of corporate perpetual capital could potentially drive credit unions to bank with other non-credit union organizations, potentially creating another corporate meltdown. The areas listed above are just a few of the concerns in the industry but not the ones that we all fear. The ones that are causing all the angst are those that allow an examiner to arbitrarily choose RBC weights or minimum risk-based ratio based upon their findings. Credit unions who, at the beginning of the exam, are considered well capitalized could by the end of the exam be immediately placed into prompt corrective action (PCA).

The NCUA has outlined areas which allow the examiner to increase minimum capital, but falls far short of describing the process for determining the number or a formula to determine how much more capital the credit union must maintain. So let us call a spade a spade. The RBC number is not about capital at all; it is about the NCUA putting a credit union into PCA so that all NCUA recommendations, regardless of whether they are to the benefit of the credit union, become backed by regulatory enforcement powers.

Regardless of the outcome of the comments submitted on the final regulation and coupled with the reality that our regulators make very few changes based upon credit unions concerns, it would be prudent to assess the risk that a rogue finding on an exam could do exactly what has been described above. Never in the history of NCUA rule-making has it been necessary to classify a regulator as a risk to the credit union. However, we are not in normal times and the NCUA's actions over the last few years are indicative of a regulator who believes they need to manage all the perceived risk out of a credit union's operations. In the coming days AuditLink, a division of CU*Answers, will be publishing a more detailed analysis/risk assessment that will discuss proactive tactics to prepare credit unions when the regulation goes wide in 18 months.

NCT



Regulation E vs. ACH 60 Day Timeframes

Cynthia J. Thompson, AAP, CTP
Director of Education & Professional Services
The Payments Authority

Back Office & Teller Line

Regulation E provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, point-of-sale (POS) terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or to debit a consumer's asset (deposit) account.

A provision of Regulation E states that if a consumer notifies an institution that an error involving an EFT has occurred, the institution must investigate and resolve the claim within specified deadlines. Errors covered by this requirement include unauthorized EFTs, incorrect EFTs, and the omission from an account statement of an EFT that should have been included.

Q. How long does the consumer have to notify us of an error on their statement?

A. In order to limit their liability, the account holder must notify the bank or credit union within 60 days of receiving the statement with the error.

Q. What if the consumer notifies us after the 60 days? We have a consumer that notified us in July that he had transactions debited every month since January.

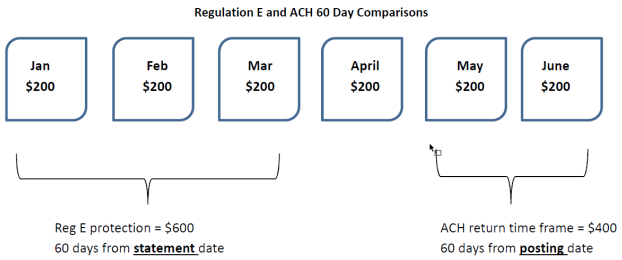
A. The consumer is always protected for the first 60 days following receipt of the statement with the first error (with the exception of failure to notify the financial institution timely of a lost or stolen card). In this case, the consumer would be reimbursed for transactions on the first statement and any transactions within the following 60 days from receipt of the statement. The consumer is liable for transactions after the 60 day period.

Q. What is the difference between the Reg E 60 day period and the ACH 60 day right of return?

A. Using the example above, the consumer would be reimbursed for transactions on the first statement and any transactions within the following 60 days, to comply with Reg E error resolution. In addition, any ACH transactions that fall within the ACH 60 day right of return can be returned by obtaining a Written Statement of Unauthorized Debit. The financial institution will absorb the loss for the Reg E period. The consumer will be reimbursed for the transactions within the Reg E period, and for any transactions returned via ACH. The consumer is liable for any transactions that posted in between the two time frames. (This does not preclude the financial institution from attempting to contact and collect from the originating financial institution (ODFI).)

Q. When does provisional credit have to be provided?

A. Provisional credit should be given no later than 10 days following the date of notice of the dispute for ATM and debit card transactions. Generally ACH transactions are returned without requiring investigation, so credit is provided when the ACH transaction is returned.



Reg E 60 days:

Using the above example, if an ACH transaction posted on January 2nd, and the statement generated on January 30th, the consumer would have 60 days from receipt of the January statement to notify the financial institution of the error. If additional transactions posted in February and March, the consumer would be reimbursed for those transactions.

continued on page 6

continued from page 5

ACH 60 days:

Assuming the consumer notified the financial institution of the errors on June 30th, the transactions that posted in May and June (no later than 60 days from settlement) can be returned through the ACH, upon receipt of a Written Statement of Unauthorized Debit. The financial institution cannot use the May and June returns to offset the loss charged off by the first transactions; the consumer must be re-credited.

Consumer Liability:

The consumer is liable for any transactions that post between the Reg E error resolution timeframe and the ACH 60 day right of return. In this example, the consumer would be liable for the April payment.

NCT

Credit CARD Act Violations

continued from page 1

under the age of 21 must have their own independent ability to pay the required minimum payments or have a cosigner, guarantor or joint applicant who is at least 21 years old that has the ability to pay and will agree to assume liability for making the payments.

Importantly, these additional requirements for members under the age of 21 apply beyond the initial opening of the credit card account. In fact, Regulation Z requires the credit union to obtain the cosigner, guarantor or joint applicant's written agreement prior to any increases in the credit limit on the account. Thus, credit unions need to have systems in place to determine which credit card accounts are held by members under the age of 21 and procedures to obtain and document the written agreement prior to the credit limit increase.

Reducing Credit Limits

On the flip side, credit unions often have disclosure requirements when reducing a member's credit limit on a credit card account. In general, a 45 day advance notice is not required as the credit union needs the ability to reduce credit limits for safety and soundness purposes. However, the reduced credit limit could be "adverse action" triggering notices under the Equal Credit Opportunity Act and the Fair Credit Reporting Act (FCRA). For example, if the credit union noticed a drop in a member's credit score during a routine review of the member's credit and wanted to reduce the member's credit limit on the credit card account – both adverse action notices would be required and the credit union would need to be sure to include the specific "credit score disclosure" information that was added the FCRA requirements by Dodd-Frank.

Conclusion

While credit unions are focused on complying with the myriad of regulatory changes – especially the CFPB's mortgage regulations – they should not lose focus of the detailed Credit CARD Act requirements in Regulation Z. And, by ensuring compliance with the existing regulations now credit unions will be better prepared for the CFPB's future changes to credit card requirements.

NCT

Word Search

C	S	U	O	I	C	I	P	S	U	S	E	L
R	E	T	U	R	N	D	P	G	S	X	Z	A
E	S	E	E	F	T	O	R	O	A	K	E	I
Q	U	A	A	L	L	I	L	M	P	V	R	C
U	E	C	S	I	S	Y	L	A	N	A	U	O
I	T	R	C	K	E	P	Y	F	R	X	S	S
R	N	Y	E	T	C	M	R	C	B	A	O	J
E	E	R	A	M	E	A	R	T	C	A	L	L
M	T	R	R	N	U	E	M	C	F	L	C	I
E	W	I	T	D	D	S	O	R	C	R	S	A
N	O	O	S	I	U	U	N	R	Y	U	I	B
T	R	T	T	A	N	L	H	O	W	L	D	L
U	K	N	T	T	R	E	L	A	C	E	R	E

Word List:

REQUIREMENT
FRAUD
SOCIAL
DISCLOSURE
ANALYSIS
RETURN
RATE
NETWORK
RISK
ACT
CONSUMER
LIABLE
PAYMENT
SUSPICIOUS
POLICY
RULE
ACCOUNT
FEES
ALERT
CREDIT
EXAM
LOSS

Let AuditLink perform your Concentration Risk Analysis

AuditLink Can

Use your native data to validate your concentration risk policy

Develop a concentration risk policy for your credit union

Validate thresholds against economic scenarios to determine capital adequacy

Generate a report for your Executive Team and Board

Perform quarterly updates to make sure you stay in policy

Get started with AuditLink today!
auditlink.cuanswers.com

AuditLink
CU*ANSWERS Management Services