Freeborn

Your Future Is Our Purpose

Freeborn's Credit Union Rules Report

by Brad R. Bergmooser

ISSUE TWO I FALL 2014

"The products and services provided to members is in a period of drastic change. Credit Unions can leverage this evolution into growth so long as they are committed to fully understanding, vetting, and implementing these new technologies."

Credit Unions, Let Me Introduce You To Apple Pay

Is Apple Pay the future of payment processing? Maybe. Are mobile payment services in general – Apple Pay, or an evolution or competitor thereof, the future of payment processing? Start planning for it.

First of all, anything with starting with "Apple" sounds intriguing, but how does Apple Pay work? In short, it takes a member's credit or debit card and assigns it a device specific "token". This "tokenization", in theory, ensures that the card information itself is not stored either on the phone or on Apple's servers. To conduct a transaction, the member's phone uses a thumbprint (called TouchID) to authenticate and begin the payment. Then the phone transmits the security token to the merchant terminal and a transaction security key will be created (this is similar to EMV transactions on plastic cards). The remainder of the transaction continues much like a traditional credit transaction and the credit union verifies that the transaction is coming from the assigned device.

The process, players, and legal structure surrounding mobile payment services likely leaves you with more questions than answers, many of which are vital considerations a credit union must make before offering such a service. Is the credit union liable for unauthorized transfers? Is the tokenization method more secure than traditional payment processing? Will Apple (or another operating system) take a cut of interchange fees and how does that impact the credit union's credit or debit card portfolio? Should our member agreements and disclosures be amended? Before signing on the dotted line to partner with Apple, or Google, or whoever is offering the latest mobile processing system, it's imperative to fully understand how the process will work and how the credit union will be impacted.

Apple Pay signifies a drastic change in how credit unions do business, but change can be very rewarding if approached correctly. Freeborn is dedicated to advising its clients on matters affecting them today, and is just as committed to assisting credit unions put the programs and services in place that they need to succeed in the future.

FFIEC is Suggesting Credit Unions Take a Closer Look at Their Cybersecurity Policies

NCUA recently issued a press release discussing the report published by FFIEC following their assessment of 500 financial institutions' cybersecurity practices. Although the document states that FFIEC's results are "observations," and they should not be taken as binding authority since FFIEC guidance already exists (contained at the end of the assessment document), given the large scope and publicity of recent merchant data breaches, credit unions should closely review and determine if they can incorporate any of FFIEC's specific recommendations.

The report separated FFIEC's findings into "Cybersecurity Inherent Risk" – what could be attacked, and "Cybersecurity Preparedness" – what to do about it. Three identified targets were:

1. Connection types. From internet service providers to having employees log in to credit union networks through personal devices. FFIEC urged an evaluation of the need for each connection type – with more access points equating to a larger chance of attack;
2. Products and services. Credit unions should have an understanding of how each product or service could be a threat to credit union operations (a criminal making unauthorized transfers using stolen debit card information, for example); and
3. Vulnerabilities associated with each technology utilized, from core processing services to physical ATMs.

While FFIEC admitted that cybersecurity policies can differ among financial institutions, it outlines the following general areas to be considered:

1. Risk Management. Cybersecurity practices should routinely be discussed at the board, management, and employee level;
2. Threat Intelligence and Collaboration. Credit unions must remain cognizant, through internal monitoring and sharing with industry partners, of sources of cyber threat;
3. Cybersecurity Controls. Credit unions should ensure their current software systems are adequate in preventing, detecting, and correcting threats. For example, credit unions may consider periodic intrusion tests to gauge exposure to cyber-attacks;
4. External Dependency Management. This issue relates to due-diligence standards in evaluating third-party vendors. Credit unions should have considerable contractual assurances of a third-party vendor's management of cybersecurity risk as well as indemnification protection; and
5. Cyber Incident Management and Resilience. This is the after the attack concern and FFIEC suggests credit unions have current disaster recovery plans amended to include potential cyber incidents.

ABOUT THE AUTHOR

Brad R. Bergmooser
Senior Counsel,
Credit Union Industry Team

Chicago Office
(312) 360-6944

bbergmooser@freeborn.com

Brad represents credit unions and other financial institutions, concentrating on regulatory compliance, and other corporate and transactional matters. He has assisted financial institutions on loan participation arrangements, mergers, and indirect lending agreements. Additionally, Brad has worked with financial services clients through all phases of development, from contracting to implementation, for mobile banking and remote deposit capture products.

FFIEC's summary of findings is not authoritative guidance, *per se*, but addressing some of its recommendations could be a sound business practice and may place credit unions at an advantage in upcoming examinations. A link to the NCUA release, inclusive of the FFIEC documents is below, and the attorneys and business advisors at Freeborn can assist in applying the general guidance materials to the specific operations of your credit union.

http://www.ncua.gov/News/Pages/NW20141103FFIEC.aspx

Other Important News

1. Are you opening accounts for marijuana businesses operating under state law? There's more than the recent FinCEN guidance to consider, and the practice remains a large risk for credit unions without clear direction from NCUA, or a unified approach across the industry: **Credit Unions Forced to Close Marijuana Accounts**

2. Fannie and Freddie appear to be pushing for lower down payment mortgages. Will your credit union's standards change? **Fannie Mae Official Details Plan to Ease Mortgage Rules**

3. Well, we knew it was coming. CFPB has issued proposed rules to regulate general use prepaid debit. More on this in a later issue! **Prepaid Products: New Disclosures to Help You Compare Options**

The CU Rules Report will be sent out periodically so our credit unions can plan, account for, and become compliant with any new rules, laws or other issues that may affect their business. In an environment of ever changing law, regulation, technologies, and other market factors, Freeborn & Peters LLP is committed to keeping its credit union clients ahead of the curve.

Thanks, and we'll talk with you soon.

Brad