A CU*ANSWERS WHITEPAPER

MARCH 2013

CREDIT UNION LIABILITY FOR ONLINE FRAUD UNDER UCC 4A

March 12, 2013

Our industry often focuses on how to manage examinations. This document, by contrast, is to help understand credit union liability to members for losses to their accounts as a result of fraud, and the best practices for protecting the institution against this risk.

CU*ANSWERS
A Credit Union Service Organization

AuditLink
CU*ANSWERS Management Services

FRAUD HAPPENS FAST

Around 11:30 a.m. on a slushy day of January 22, 2009, fraud analysts at Comerica Bank received a call. Apparently one of Comerica's clients, Experi-Metal, Inc. (EMI), had dozens of suspicious wire transfers draining money from EMI's accounts to banks located in Russia and Estonia. EMI was contacted to find out whether any of the transfers were legitimate. As it turned out, of course, *none* of the transfers was legitimate. Around noon, Comerica's fraud team got the frantic message to shut down EMI's access credentials. EMI's credentials were disabled, but there was a terrible error made by Comerica personnel. Although disabling the account prevented anyone from logging in, it did not remove anyone *currently* logged in from continuing to transfer money out of the account. For the next two hours, the criminals using EMI's credentials continued to steal funds before Comerica realized the problem and finally shut the account down for good. During the six hours the European thieves had access to EMI funds, ninety-three fraudulent transactions had been processed by Comerica, totaling almost two million dollars. Working with domestic and international banks, Comerica was able to recover some funds, but half a million dollars was permanently lost.

After investigating the incident, it turned out that EMI was the victim of a phishing attack where criminals from Eastern Europe sent emails to Comerica customers, taking them to a false web page. In the early morning of January 22nd, the VP of Manufacturing for EMI forwarded just such an email to the company controller. The email was entitled "*Comerica Business Connect Customer Form*" and had a link to a webpage. The controller clicked on this link and promptly entered his confidential secure token identification, Treasury Management Web ID, and login information. This instantly gave the criminals access to EMI's accounts. With no hope of recovering the half million stolen by the Eastern European thieves, EMI made a demand on Comerica to make good on the losses. Comerica, citing EMI's own negligence, refused. EMI then sued Comerica for the lost funds. Comerica immediately filed a motion for *summary judgment* (a request for the court to find in their favor prior to a trial and dismiss the case).

The key questions facing the court were whether EMI should win outright, or if Comerica should have the case e case should be dismissed here, or whether to continue the proceedings towards trial. In its opinion, the court relied on §4A of the Uniform Commercial Code (UCC 4A), which governs the laws of online transactions between consumers and financial institutions. Applying the law of UCC 4A, the court ruled that Comerica was potentially liable for the loss, but that EMI would still need to go to trial. (EMI and Comerica eventually settled for an undisclosed sum before trial). In the analysis of who bore liability, the actions of EMI were *irrelevant*, even though without EMI's blunder in providing credentials to the European thieves there would not have been any losses. Instead, Comerica had the burden under UCC 4A of showing that the bank had commercially reasonable security and processed the transactions in good faith. These UCC standards of commercial reasonableness and good faith apply to all financial institutions and are used in litigation to determine who will prevail when a consumer loses funds through online fraud. ◆

WHAT IS THE UNIFORM COMMERCIAL CODE?

The Uniform Commercial Code (UCC) is not a federal law, but rather a model set of rules. The purpose of the UCC is to create uniformity in laws governing sales and other financial transactions between all 50 states. While there may be some differences as each state legislature modifies its own Commercial Code to meet certain needs, generally the rules remain very similar as each state reviews the UCC and its updates.

For financial institutions, §4A of the UCC (UCC 4A) is extremely important as this section governs funds transfers. Most states have adopted UCC 4A without any change to the language. UCC 4A defines *commercially reasonable security* and provides the framework as to when a credit union will be liable for the loss of funds due to online fraud. ◆

WHO WINS IN A UCC 4A CIVIL LITIGATION BETWEEN A CONSUMER AND A CREDIT UNION INVOLVING ONLINE FRAUD?

STEP ONE: IS THIS A UCC 4A DISPUTE?

Is this a case involving an online transaction fraud requiring a security process?

JUDGE DECIDES

✗

IF NO

CREDIT UNION WINS

✓

IF YES

GO TO STEP TWO

STEP TWO: DID THE FRAUD ORIGINATE FROM THE CONSUMER OR THE CREDIT UNION?

Was the fraud due to error or security breach by credit union, and not the consumer?

JUDGE DECIDES

✓

IF YES

CONSUMER WINS

✗

IF NO

GO TO STEP THREE

STEP THREE: WAS THE SECURITY OF THE CREDIT UNION COMMERCIALLY REASONABLE?

Given the following four factors (the wishes of the consumer, circumstances of the consumer, alternative security procedures offered by the financial institution, and the security procedures in use by the financial institution's peers) was the security commercially reasonable?

JUDGE DECIDES

✓

IF YES

SKIP STEP FOUR

GO TO STEP FIVE

✗

IF NO

GO TO STEP FOUR

STEP FOUR: DID THE CONSUMER AGREE TO A LESS SECURE PROCESS?

Did the credit union offer commercially reasonable security for the consumer that the consumer rejected, and that the consumer agreed in writing to be bound by the transactions processed by the less secure process?

JUDGE DECIDES

✓ **IF YES**

GO TO STEP FIVE

✗ **IF NO**

CONSUMER WINS

STEP FIVE: DID CREDIT UNION PROCESS THE TRANSACTIONS IN GOOD FAITH?

Did the financial institution accept the transactions in good faith, meaning that (a) the credit union followed its procedures, (b) was not dishonest in processing the transactions, and (c) by processing the transactions met commercially reasonable standards of fairness?

JURY DECIDES

✓ **IF YES TO ALL**

CREDIT UNION WINS

✗ **IF NO TO ANY**

CONSUMER WINS

To recap, the **consumer wins** in a UCC 4A online fraud case *if*:

The security procedure was *not commercially reasonable*, or

Even if commercially reasonable (or the consumer agreed to be bound by a less secure procedure), *consumer still wins* financial institution does not accept the transactions in *good faith*, meaning the credit union failed to meet its own procedures, had dishonesty by it employees, or by a failure to respond to the transactions in a commercially fair way. ◆

BEST PRACTICES FOR CREDIT UNIONS

Because even a negligent client can recover for a loss of funds through online fraud, credit unions should follow a few key practices to lower the risk of liability.

1. Maintain up-to-date security on all machines involved in the processing of online transactions.

2. Complete risk assessments on an annual basis and avoid taking a "one size fits all" approach to security. Ensure commercial clients or members who engage in large transactions receive special attention with respect to security.

3. Keep up to date with the security processes employed by peer institutions, and remain up to date with FFIEC, NCUA, and state regulations regarding online transaction security.

4. If a member rejects a higher level of security in favor of a riskier, less secure method, ensure that the member signs a writing indicating that the member understands there is greater risk and that the member agrees to be bound by the transactions processed through the riskier method (the writing should directly refer to the applicable state UCC 4A language).

5. Conduct audits to ensure credit union employees are following policies and procedures for online transactions, especially high risk transactions such as wire transfers and ACH.

6. Review online banking accounts on a regular basis for abnormal activity.

7. Provide explicit instructions to employees on what to do if fraudulent activity is suspected.

While it is true that the standard of care used by the credit union is irrelevant in a UCC 4A case, there are two good reasons to follow these best practices. First, by following the best practices there is less chance of having a breach of security resulting in financial institution liability. Second, the standard of care employed by the credit union *is* important in a negligence case. A credit union that is negligent could fare far worse than a UCC 4A claim, because a consumer who wins a negligence case may be entitled to punitive damages. ◆

OTHER CONSUMER AVENUES OF RECOVERY

Even a credit union that otherwise prevails on UCC 4A claims could still potentially lose on breach of contract, negligence or violation of other statute or regulation. A credit union could still be liable where the credit union breaches a common-law duty to safeguard the assets of its consumers. A credit union could also be liable for the mental anguish and other suffering brought on by the incident. A plaintiff might voluntarily abandon a UCC 4A claim and pursue the credit union for common law negligence which could result in punitive damages against the credit union.

There are certain states that recognize the doctrine of *negligence per se*, where violation of a statute that pertains to the subject matter at issue changes the burden of proof from the plaintiff consumer to the defendant financial institution making consumer recovery more probable.

Of course, the same best practices that a credit union can use to protect itself from UCC 4A claims are also defenses to negligence. ◆

COMMERCIAL REASONABLENESS

In order to prevail in a civil lawsuit where consumer funds were lost through online fraud, a credit union must show the security of the online transactions was *commercially reasonable*, and that the credit union processed the transactions in *good faith*. Financial institutions need to be aware that the strict liability imposed by the UCC means close questions in the proceeding will likely be resolved in the consumer's favor.

For a credit union to have any chance to prevail, online fraud must result from the consumer's actions. If the fraud results from actions by the credit union the consumer will win, such as a case where malware was installed on a credit union workstation. Note that for the purposes of commercial reasonableness, *it does not matter how careful the credit union is in preventing online fraud in its organization.* Strict liability means that the credit union is *always* liable to consumers no matter how careful the institution was, if the fraud occurs through no fault of the consumer.

Commercial reasonableness is a question of law, meaning that in any litigation the judge and not the jury will decide what constitutes commercial reasonableness. In effect, whether or not security is commercially reasonable will probably be litigated in front of a judge prior to a trial.

The definition of and facts a credit union can use to prove commercial reasonableness can change over time. The language in UCC4A is specifically designed to change as technology changes and new threats emerge in online banking. This also means that what was commercially reasonable in 2009 might not be so in 2013 and the commercially reasonable solution in 2013 may no longer be so in 2015. ◆

FOUR FACTOR TEST FOR COMMERCIAL REASONABLENESS

UCC4A(c) lays out the four factors a judge may consider when determining the commercial reasonableness of a security provision:

1. The wishes of the consumer

2. Circumstances of the consumer (the size, type and frequency of payment orders)

3. Alternative security procedures offered by the financial institution

4. Security procedures in use by the financial institution's peers

No one factor here is more important than another, and the judge is allowed to consider every factor in issue. Notice too, that this a consumer-by-consumer analysis rather than a one size fits all approach.

Note: This is an area where a good lawyer or law firm can really earn their fees by researching and using persuasive facts to prove commercial reasonableness on behalf of the credit union.

In the *Comerica* case, the judge ruled that the bank did indeed have commercially reasonable security for EMI, but that Comerica may have failed in its good faith duties to the consumer, and set a trial to determine if this was true. Had Comerica not used commercially reasonable security, EMI would have won the case outright. ◆

SAFE HARBOR FOR COMMERCIAL REASONABLENESS

If all of the following circumstances are present:

1. The financial institution offers commercially reasonable security for the consumer, and

2. The consumer rejects that offer in favor of a less secure method of processing the transactions, and

3. The consumer agrees in writing to be bound by transactions processed by the less secure method,

Then the less secure method is *automatically assumed to be commercially reasonable for that consumer* **if** the financial institution accepted the payment order in good faith.

For example, if a credit union normally does not allow a credit card transaction to be processed overseas, and the member wishes that security function to be disabled, as long as the member agrees in writing to be bound by these overseas transactions the credit union is not liable for not having commercially reasonable security.

The credit union will still need to make a showing before the judge that the credit union had a commercially reasonable solution that was rejected in favor of a less secure method. For example, if a credit union develops a mobile banking application that is less secure than its online banking solution, the credit union probably cannot take refuge in the safe harbor provisions of UCC4A. (The mobile banking application is not commercially reasonable). However, if the consumer is offered a mobile banking application solution with commercially reasonable security that the member demands be turned off, as long as the credit union has a writing from the consumer the solution will be deemed commercially reasonable for *that consumer.* ◆

EXCERPT OF UCC4A

§ 4A-202. AUTHORIZED AND VERIFIED PAYMENT ORDERS.

(b) If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted.

(c) Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated.

A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer. ◆

REQUIREMENT OF GOOD FAITH

The definition of what constitutes "good faith" in processing the transactions can be found under UCC 4A-202(b). Good faith requires the credit union to have honesty in fact and the observance of reasonable commercial standards of fair dealing.

1. "Honesty in fact" asks whether the financial institution knew as a factual matter that the transaction was unauthorized, and yet still processed the transactions.

2. "Reasonable commercial standards of fair dealing" imposes an additional standard, i.e. whether the individual's actions were consistent with commercially reasonable standards of fairness.

3. Good faith also requires that the financial institution actually followed through on its security procedures.

The burden of proof is on the financial institution to show all elements of good faith if the credit union processes an unauthorized transaction.

Honesty in fact is relatively simple: as long as no employee acts dishonestly in accepting the transfers, the financial institution has met this prong of the definition. In other words, the credit union is liable if employees know the transactions are fraudulent but processes them anyway.

The definition of reasonable commercial standards is more complex and is best understood by reviewing the facts in the *Comerica* case. EMI used four arguments to claim that Comerica failed to meet good faith requirements:

1. Comerica failed to institute additional security procedures that would have enabled it to detect the unusual activity with EMI's account.

2. Comerica allowed thieves to initiate 47 wire transfers even though EMI had only initiated two wire transfers in the previous two years (and both of those transfers came a full two years before those initiated by the thieves in this case).

3. Comerica failed to be alerted to the fraudulent nature of the wire transfers based on the unusual destinations of those transfers (e.g. Moscow, Estonia and China).

4. Comerica allowed the initiation of 46 additional wire transfers *after* being instructed by EMI that Comerica should not honor any more wire transfers.

The court rejected EMI's first argument (Comerica was said to have "commercially reasonable security") but accepted the rest as potentially valid. The court found that EMI's other arguments raised the possibility that Comerica did not act in good faith, and therefore should be adjudicated at trial.

Note that EMI's arguments simply kept the case going; they might not have prevailed if this case had gone to trial instead of settlement negotiations. ◆

STRICT LIABILITY FOR FINANCIAL INSTITUTIONS UNDER UCC4A

The UCC imposes strict liability on financial institutions that fail to satisfy the UCC's requirements. This means that the credit union fails to meet UCC standards, the credit union will be responsible for all funds lost by the consumer. ◆

ROLE OF THE FFIEC

The FFIEC has developed two key compliance Guidance manuals, the *Authentication in an Internet Banking Environment* (2005) and its *Supplement* (2011). While compliance with these FFIEC Guidance rules is mandatory, in a court of law compliance or non-compliance with FFIEC will not be dispositive. However, compliance with FFIEC is very important as these Guidelines will certainly be entered into evidence. In addition, federal and state regulatory agencies can punish credit unions for non-compliance with FFIEC Guidelines, irrespective of a civil case disposition. ◆

ROLE OF THE NCUA AND STATE REGULATORY AUTHORITIES

In most states, compliance review documents are inadmissible in a civil proceeding and are not subject to discovery. Exam results are also protected by law and cannot be discovered in litigation. Indeed, if the credit union turns over this information voluntarily, it may be subject to sanctions by a regulatory authority. NCUA employees are exempt from testifying or providing evidence under 12 C.F.R. PART 792.

However, a credit union may be able to submit other documents created by a regulatory agency, such as the Aires IT Questionnaire, and offer evidence to prove commercial reasonableness of the credit union's security. ◆