The Commercial Reasonableness of Bank ACH Security Procedures

Stan Stahl, Ph.D.
Brad Maryman

Introduction

One sunny morning in late June, Sally, the payroll manager at A-Logistics, a mid-sized distribution and transportation company, received an email identified as being from Facebook.[1] The email informed her that a friend from Junior High School had written on her wall. Sally clicked the link in the email which took her to her wall but she was disappointed to see that her wall was empty. Disappointed, she chalked it up to a problem with Facebook and returned to her job of preparing that week's payroll database for transmission to the company's bank. What Sally didn't know was that when she clicked that link in her email she was not only taken to Facebook. Clicking that link installed a notorious malware program called Zeus on her computer. Fewer than 50% of Zeus variants are detected by anti-virus programs.

Ten days later cyber criminals, logging onto the bank using A-Logistics' UserID and password, transferred $750,000 from the company's payroll account to 90 waiting money mules across the United States. In less than 24 hours all but $150,000 of the money had been sent to Eastern Europe.

During the 10 days prior to the theft, Zeus had been silently recording all of Sally's keystrokes and sending them to the cyber criminals, including the UserID and password to access A-Logistics' online banking. Using Zeus as a backdoor into Sally's computer, the cyber criminals had found other payroll files which they were able to use as a template. It was, as the saying goes, as easy as taking candy from a baby.

A-Logistics notified their bank immediately upon discovering the fraud, requesting the return of their money. The bank informed A-Logistics the responsibility was entirely A-logistics'; that it had no responsibility in the matter since the bank employed commercially reasonable security procedures. A-Logistics sued its bank to recover the stolen money.

Our expert opinion after reviewing the bank's security procedures on behalf of plaintiff was that the bank's security procedures were in fact not commercially reasonable.

[1] The company name is fictitious and the industry has been changed. The story, including our findings, is true.

Why This is Important

Our story is not unusual. Banks have seen an epidemic increase in online bank thefts as the sophistication of cyber criminal attacks has not been met by a corresponding increase in defenses. Quite frankly, the situation is so bad that a bank would not be remiss to assume that the human on the other end of the electronic transaction is not its customer. [2]

The situation is analogous to the classical Dutch story of the little boy putting his finger in the dike to stop the water; only now the water threatens to overwhelm the little boy. Now is the time for everyone – including financial institutions – to do their part.

The egregious extent to which the security procedures of the bank we reviewed failed to be commercially reasonable should be a clear indication that every bank has opportunity to make its own security procedures more commercially reasonable.

By better managing the commercial reasonableness of its ACH security procedures, a bank will realize several benefits:

1. Lower the likelihood that its customers will be victims of online bank fraud, even in the presence of compromised customer computers
2. Lower the likelihood that it will be sued for online bank-fraud losses
3. Improve its ability to successfully withstand a lawsuit to recover online bank fraud losses
4. Improve its loss history and potentially lower its insurance costs
5. Increase customer satisfaction as customers come to know and appreciate that the bank "has its back"
6. Gain competitive advantage

There is also community benefit. To the extent that non-commercially reasonable ACH security procedures contribute to online bank fraud, these procedures impact the financial system. Therefore, improved ACH security procedures can be expected to have two significant benefits to the entire financial system.

1. Lower the incidence of online bank fraud
2. Increase confidence in the financial system

With the above in mind, the purpose of this article is to share our findings with the banking community, giving banks the information they need to assess and strengthen their ACH security procedures.

[2] For an overview of the seriousness of the problem see the postings indexed under "Financial Systems Security" on http://blog.citadel-information.com.

Uniform Commercial Code Definition of Commercial Reasonableness

Uniform Commercial Code – Article 4A, Part 2 governs the issue and acceptance of payment orders as part of the funds transfer process. We have extracted below relevant sections of the UCC as defining and establishing the conditions for "commercial reasonableness" and have italicized the section of § 4A-202 (c) where "commercial reasonableness" is defined. [3]

§ 4A-201. SECURITY PROCEDURE.

"Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.

§ 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.

(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.

[3] Our text of the Code is from Cornell University Law School, http://www.law.cornell.edu/ucc/4A/4A-202.html.

As can be seen, determining the commercial reasonableness of a bank's security procedure means analyzing the extent to which, for every ACH transaction, the bank's security procedures as applied to that transaction consider:

1. The wishes of the customer as expressed to the bank
2. The circumstances of the customer known to the bank, including the transactional criteria such as size, type, and frequency of payment orders normally issued by the customer to the bank
3. Alternative security procedures offered by the bank to the customer
4. Conformance with security procedures in general use by customers and receiving banks similarly situated [4]

This means, in particular, that it is not the general question of the bank's security procedures as they are in general use but the specific question of the bank's security procedures as applied to a specific transaction (or set of transactions). It is not enough to have great security procedures in principal; a bank must correctly instantiate its security procedures on each and every ACH transaction. If not, then plaintiff may be able to assert that the bank's security procedures on the fraudulent transactions were not commercially reasonable.

Our Findings Established That Bank Security Procedures Were Not Commercially Reasonable

The security procedures followed by the bank in accepting the fraudulent ACH files overrode the known wishes of A-Logistics as agreed with by the bank.

The bank overrode three specific agreements it had with A-Logistics.

Agreement to Provide Dual Control Protection

A-Logistics and the bank agreed in August 2007 that the bank would implement Dual Control protection for A-Logistics in January, 2008. However the bank converted to a new online bank system in the Fall, at which time it unilaterally dropped the requirement for Dual Control. In our review of bank and A-Logistics documentation, we saw no evidence that the bank ever notified A-Logistics of this change with the result that Dual Control was not in place for the fraudulent ACH transactions.

[4] We've not included the final sentence of § 4A-202 (c) where the customer over rides the security procedures offered by the bank as this acts as a "get out of jail free card" for the bank. This conforms to the paper's primary objective of focusing on the bank's responsibility to assure it meets the italicized portions of § 4A-202 (c).

Agreement to Provide Enhanced Log-in Security Procedures

The Bank's standard *Online Banking Agreement* states that the bank has implemented and will follow certain *Enhanced Log-in Security* procedures for customer authentication to include scrutiny of the user's IP address; Internet Service Provider; PC and browser settings; time of day and geographic location.

Even as the bank promised to "scrutinize" these elements, the user's IP address; Internet Service Provider; time of day and geographic location were ALL different on the $750,000 fraudulent transaction. Furthermore, in our review of the transaction audit logs provided to us by the bank, we saw no indication that the bank even captured PC and browser settings.

The above alone would have been adequate to support a contention that the bank failed to abide by its *Online Banking Agreement*. But there's more …

Based on bank documentation, the bank's *Enhanced Log-in Security* is based upon a *Risk Based Authentication* technology which monitors every ACH transaction. [5] Technology like this, if properly implemented, would go a long way towards meeting the standard of commercial reasonableness. However, based on deposition testimony from a bank employee, the bank was not even using this technology to monitor transactions during the period when the fraud occurred.

Agreement to Notify A-Logistics before Accepting Large ACH Transactions

The Agreement: A-Logistics and the bank had agreed that the bank would contact A-Logistics for its approval before the bank would approve an ACH transaction greater than $500,000.

What Happened: The $750,000 ACH transaction in question generated an alert to management that the transaction amount was of a sufficiently high amount that it needed a Vice President's approval before the bank could accept it. Thus an email was sent to a VP for approval. That VP replied that the amount above his signature authority and forwarded it a Senior VP. This Senior VP then approved the transaction.

Nowhere in this sequence of emails was there any mention that, perhaps, A-Logistics had an interest in the ACH transaction. Operations, a VP and a Senior VP followed the bank's

[5] According to the vendor: "*Transaction Monitoring is an online risk management system specifically designed to optimize fraud investigation resources by pinpointing high-risk online banking activities in real-time. Through RSA's Risk Engine, Transaction Monitoring detects, analyzes, and scores each online banking activity. Transaction Monitoring also utilizes information gleaned from RSA's eFraudNetwork – a cross-bank, cross-application, cross-border online fraud network – to pinpoint fraudulent activities. A decision engine then determines which actions should be executed, depending on the calculated risk score together with numerous other parameters."*

procedures in accepting the transaction. *Each of them had the opportunity to follow the known wishes of A-Logistics as agreed to by the bank. Yet none of them did.*[6]

The security procedures followed by the bank in accepting the fraudulent ACH transactions failed to consider the circumstances of the customer known to the bank, including transactional criteria such as size, type, and frequency of payment orders normally issued by the customer to the bank.

Our review of the bank's procedures in accepting the fraudulent $750,000 ACH transaction identified eight different independent ways in which the bank failed to consider the circumstances of the customer known to the bank, including the transactional criteria such as size, type, and frequency of payment orders normally issued by A-Logistics to the bank.

1. The ACH batch file database name was unusual and was established during the same session as the fraudulent ACH batch file was sent. A-Logistics previous history was to create the ACH batch file the day prior to when it was sent.
2. The ACH batch file was submitted on Friday; A-Logistics customarily submitted its ACH payroll file on Tuesday.
3. The ACH batch files were out of sync with the customary and usual frequency of ACH batch files sent by A-Logistics.
4. The ACH batch file directed payments to numerous payee accounts to which A-Logistics had never before transferred funds.
5. The ACH batch file transfer originated from IP addresses that A-Logistics had not previously used to conduct its online banking.
6. The ACH batch files originated from an Internet Service Provider different from A-Logistics' ISP
7. The ACH batch files originated from a geographic location different from A-Logistics' geographic location.
8. The login credentials used for the fraudulent ACH transaction had never before created a new payment database nor had ever before logged-in from that IP address.

Had the bank missed one or two of these differences one might argue that its security procedures as applied to the transaction in question were still commercially reasonable; after all "commercially reasonable" does not require perfection. However, this argument pales against the reality that (i) it missed eight distinct differences between the normal circumstances of A-Logistics ACH payroll transactions and (ii) had it caught even one of these different circumstances, the fraudulent transaction would not have been accepted.

[6] Perhaps ironically, when the VP at the bank with responsibility for A-Logistics' business with the bank was informed of the ACH transaction he immediately alerted the bank that it was fraudulent. But by then, the horse had left the stable.

The bank offered no alternative security procedures to A-Logistics even though A-Logistics asked for them and the bank had the technology in place to offer alternative improved security procedures.

Our review of a series of emails documented that A-Logistics had asked the bank to provide additional security by blocking transactions from unapproved IP addresses. The bank had told A-Logistics that it could not block all IP addresses except those belonging to A-Logistics. However it did not tell A-Logistics that the bank could block all IP addresses whose first 3 IP block ranges differed from A-Logistics'. Had the bank informed A-Logistics of this available alternative and allowed them to take advantage of it, the result would have been to have blocked the fraudulent ACH payment order transaction.

While this has no direct impact on the court's decision on whether or not the bank's security procedures were commercially reasonable, a court might choose to indirectly use the facts that (i) A-Logistics asked for additional security and (ii) the bank failed to tell A-Logistics that it had additional security available as added factors in determining that the bank's security procedures were not commercially reasonable.

Commercial Reasonableness May Be Inadequate Defense

The UCC's final criteria of commercial reasonableness — conformance with security procedures in general use by customers and receiving banks similarly situated — would seem to be a broad shield against bank liability; after all, if this bank's security procedures are no worse than other bank's then why should this bank be liable?

While UCC accepts what is in "general use" as an element of its standard of "commercial reasonableness," plaintiff may offer two precedents to a court to impose a higher standard of reasonableness whether such standard is in general use or not. [7]

In the first precedent, 189 U.S. 468, 470, 1903, *Texas & P.R v Behymer*, Supreme Court Justice Oliver Wendell Holmes wrote: *"[w]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not."*

In the second precedent, 60 F.2d 737 2d Cir., 1932, *T. J. Hooper v. Northern Barge*, Justice Learned Hand wrote *"Indeed in most cases reasonable prudence is in fact common prudence;*

[7] See for example, *An Emerging Information Security Minimum Standard of Care*, Robert Braun, Esq., Stan Stahl, Ph.D., in *Information Security Management Handbook, Fifth Edition*, edited by Hal Tipton and Micki Krause, Auerbach, 2005 and *An Emerging Information Security Minimum Standard of Care*, Robert Braun, Esq., Stan Stahl, Ph.D., in *Privacy and Security Law Journal,* March 2006.

but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices … Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."

Below are three illustrations of how plaintiff might use these precedents to argue against a bank's procedures being commercially reasonable, even when they are used by most similarly situated banks.

Illustration 1: Bank fails to follow regulatory recommendations

The bank failed to act in accordance with recommendations made by the *Federal Financial Institutions Examination Council* (FFIEC). In October 2005 the FFIEC published a document entitled "Authentication in an Internet Banking Environment." The document calls attention to increased opportunities for online bank fraud and concludes as follows:

> Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. *Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.* [8]

While not a bank requirement, the recommendation is clear. Banks should conduct a risk assessment and, where warranted, implement second-factor authentication.

If most similarly situated banks have implemented FFIEC recommendations, then a bank's failure to do so would establish that its security procedures were not of a kind in general use. This would add additional confirmation that the bank's security procedures were not commercially reasonable.

Suppose conversely that most similarly situated banks have not yet implemented the FFIEC's recommendations. Plaintiff may still bring both *Texas & P.R v Behymer* and *T. J. Hooper v. Northern Barge* to the Court's attention that, in light of the FFIEC recommendations, they may apply to the current situation.

[8] The document is available at http://www.ffiec.gov/press/pr101205.htm.

Illustration 2: Bank fails to follow its own security procedures

As we described above, the bank, in failing to notify A-Logistics together with its failure to implement dual control protection and enhanced log-in security procedures, failed to follow its own security procedures.

Certainly if most similarly situated banks do follow their own security procedures, then the fact that the bank failed to follow its own security procedures singularly establishes that the bank's security procedures were not of a kind in general use (and, therefore, further confirms that the bank's security procedures were not commercially reasonable).

However, even if most similarly situated banks were to fail to follow their own security procedures, one would reasonably expect a court to use *Texas & P.R v Behymer* and *T. J. Hooper v. Northern Barge* to conclude that any test for commercial reasonableness include at a minimum that a bank's security procedures *as implemented* comply with its security procedures *as documented*.

Illustration 3: Bank uses demonstrably flawed security procedures

Four minutes prior to the log-on during which time the fraud occurred, someone attempted to log-on to the bank from IP address abc.def.ghi.jkl. [9] That log-on attempt was denied because of a failed answer to a security challenge question.

Four minutes later, there was another attempted log-on from the exact same IP address. This time no security challenge question was asked. It was during this session that the fraudulent transaction occurred. [10]

If most similarly situated banks having blocked a log-on attempt from an unknown IP address because an error in answering a security question would not permit a log-on from that same IP address four minutes later without asking a security challenge question of the person attempting to log-on, then the bank's failure to do so establishes that its security procedures were not of a kind in general use (and, therefore, further confirms that the bank's security procedures were not commercially reasonable).

Even if most similarly situated banks would also have allowed this second log-on attempt without asking a security challenge question, both *Texas & P.R v Behymer* and *T. J. Hooper v. Northern Barge* may very well apply to the current situation: any test for commercial reasonableness necessarily includes a requirement that a second attempted log-on coming less

[9] We've masked the real IP address.

[10] Recall from the above that this IP address is different from A-Logistics IP address.

than five minutes after a failed log-on attempt from the same IP address be subject to no less rigor than was the first failed log-on, particularly when the IP address is one that has never before been associated with that bank customer.

Steps to Achieving Commercial Reasonableness

Our review of bank ACH security procedures identified the following as *root causes* of the bank's failure to properly protect A-Logistics from online bank fraud.

1. Technology was improperly implemented, instrumented, maintained and used (ACH transaction monitoring, for example)
2. Management silos resulted in the absence of an end-to-end risk-based perspective
3. No one at the bank had a total perspective on which to make sure that security procedures were commercially reasonable

With the above *root causes* in mind, there are certain steps that a bank wishing to ensure that its ACH security procedures are commercially reasonable might take.

1. Make someone explicitly responsible and accountable for managing the commercial reasonableness of the bank's ACH security procedures
2. Review all technology platforms for their *integrated* ability to identify transactions as being high risk for online fraud; make sure these systems are correctly implemented, instrumented, monitored and used
3. Analyze the bank's total end-to-end process for approving or rejecting ACH transactions; identify all cross-functional process relationships, including IT, operations, risk, etc; re-design the approval / rejection process, as appropriate, to ensure it meets the standard of commercial reasonableness.
4. Conduct an online bank fraud risk assessment, triaging bank customers into those at high, medium and low risk. A bank may wish to consider a two-dimensional or greater grid in analyzing risk: two dimensions, for example, might be (i) how much money is available for a given customer to transfer and (ii) how likely is the given customer to be targeted for online fraud. [11]
5. Starting with high risk customers, review all customer agreements, ensuring that these are properly incorporated into the bank's approval / rejection process; review all regulatory and other recommendations, implementing these as appropriate and documenting their lack of appropriateness should that be the case; review all requests for additional security and implement these as possible

[11] There is an opportunity here for the banking industry to develop a communal intelligence system for online bank attacks. This would allow banks and law enforcement to gain a more holistic perspective on evolving threats, targets, techniques, etc. A bank could use this industry-wide intelligence system as a factor in identifying the likelihood that a given customer is a target for online fraud

6. Develop a set of performance metrics and a management "dashboard" to facilitate management of the security reasonableness of its ACH security procedure
7. Apply a continuous improvement model (like Total Quality Management, 6-sigma, etc) to continuously improve the bank's ability to distinguish online bank fraud attempts from legitimate ACH transactions.

Financial institutions that establish a rigorous management system in accordance with these seven key steps have the opportunity to significantly improve the commercial reasonableness of their ACH security procedures. The result: a lowered incidence of online bank fraud with all the benefits we noted above, both for the bank and the community.

Stan Stahl, Ph.D. is President of *Citadel Information Group*. Citadel provides information security management services to business and the not-for-profit community. An information security pioneer, Stan's background includes securing teleconferencing at the White House, databases inside Cheyenne Mountain and the communications network controlling our nuclear weapons arsenal. A frequent speaker and writer on cyber security, Dr. Stahl serves as President of the Los Angeles Chapter of the *Information Systems Security Association*. Dr. Stahl earned his Ph.D. in Mathematics from The University of Michigan.

Brad Maryman is an experienced investigative and computer forensics consultant. Prior to founding *Maryman & Associates* in 2001, he served as a Supervisory Special Agent with the *Federal Bureau of Investigation* (FBI) for over 29 years. During that time, Mr. Maryman conducted and supervised investigations, served as an Information Systems Administrator and Security Programs Manager. While at the Bureau he served as Chairman and Member-at-Large of the advisory board to the Director of the FBI on computer and information systems. Mr. Maryman has testified extensively in criminal and civil matters and provided depositions and affidavits in support of civil litigation efforts.