Dinsmore&Shohl LLP
ATTORNEYS

Is Your Bank's Security System Adequate?

March 2, 2010

Jacob A. Manning

***As seen in the February 26th issue of *The State Journal*.**

Statistics regarding payment systems in the United States are by now well-known. Check usage hit all-time highs in the 1990s, but has been on the decline since. Meanwhile, debit card, credit card, and electronic or automated clearing house (ACH) payments have sky-rocketed. Online banking has increased substantially, as customers have become more familiar and more comfortable with it.

Unfortunately, as with any other advance in bank technology, the fraudsters seem to have adapted the fastest to this change. When check fraud became more complicated and less fruitful, the focus turned to electronic payments. The Internet--and the ease with which millions of potential victims could be reached--even brought back an old standard in a new form: so-called "419" or "Nigerian" scams.

The problem for banks has always been the same: taking into account what frauds are fashionable today, what security measures must or should banks take in response? The answer is the same: commercially reasonable procedures, but what does "commercially reasonable" mean? A new case in Texas may shed some light on the subject, and it is certainly worth some attention, no matter how advanced a bank's security procedures are.

In November 2009, over the course of two days, thieves made 47 ACH transactions and 17 wire transfers totaling $801,495 from accounts held at PlainsCapital Bank, a $4.4 billion bank headquartered in Dallas. The accounts were held by Hillary Machinery, Inc., a Texas-based business, which discovered the transactions quickly. Nearly $600,000 was recovered within approximately one week, but the remainder has never been recovered and the parties dispute which party is liable for the remainder.

PlainsCapital took the unusual step of filing a lawsuit in late December to ask a federal court to declare its security procedures commercially reasonable and that it processed the wire transfers in good faith. The bank alleges that the transactions were initiated using Hillary's valid online banking credentials and that the fraud was a result of Hillary's failure to keep secure its own user and password information.

Hillary responded last week with its own claims against PlainsCapital regarding its security measures. It claims that PlainsCapital's measures are not commercially reasonable, because those measures include only user identification, password, and a secure access code. Hillary complains that PlainsCapital should have used a multi-factor security system--as do other major banks--which would have required image or word recognition, challenge questions, single-use access codes, or computer terminal authorization procedures. Hillary cites the Federal Financial Institutions Examination Council's guidance, "Authentication in an Internet Banking Environment," to support that multi-factor security was necessary.

More pointedly, Hillary notes that had PlainsCapital simply used IP address verification or geo-location information, the fraud would have been discovered. Ignoring that some of the transactions occurred on a Sunday when Hillary was not open for business, the request for an authorization code came from a

computer with an Italian IP address, and the wire transfer requests were made from a Romanian IP address--places where Hillary does not do business.

Many banks have already instituted the systems that Hillary claims were necessary, while others are undoubtedly quietly concerned that their security systems may be inadequate. Either group can learn something from the case, though.

Those banks that have less than state-of-the-art security systems should consider whether their systems employ even the basic protections. Does the system monitor access behavior? In other words, would it have caught that a transaction by Hillary originating in Romania was unusual? Does the system monitor transaction value for unusual amounts (such as $800,000 over the course of two days for a small business)? If the system has those protections, is someone assigned to monitor them? Beyond those basic protections, banks should consider the type of account, the customer's business, and the customer's requests, among other things, to determine what measures are necessary.

Even banks that employ more sophisticated security systems should take note of the case, though. Hillary alleges statistics which show that as many as 90% of computers are infected by some form of malware. Given that protecting against such infections requires substantial resources, Hillary alleges banks should be required to assume that all computers are infected, and create security systems accordingly. The pressure is, of course, always on banks to upgrade technology to meet the fraudsters' gains, but all banks should pay particular attention to developments such as this case, so that they have additional guidance as to specifically what measures are commercially reasonable.