Fraud Responsibility: Revamp the Rules?

Why PATCO Attorney Wants Key Provision Dropped

By Howard Anderson | November 13, 2013

One key provision of Article 4A of the Uniform Commercial Code, which deals with reasonable security measures for banks, needs to be dropped, contends attorney Dan Mitchell, who represented PATCO Construction in a high-profile account takeover dispute.

Article 4A, which all states have adopted, is an attempt to allocate risk between banks and their commercial customers when electronic fraud occurs, Mitchell explains in an interview with Information Security Media Group (transcript below).

The courts vary widely in their interpretation of Article 4A. The measure played an important role in the PATCO Construction case, when an appellate court reversed a lower court ruling that favored the former Ocean Bank, now part of People's United Bank, describing the bank's security procedures as "commercially unreasonable." The case was eventually settled out of court (see: PATCO Fraud Dispute Settled).

Under Article 4A, which dates back to the 1980s, a bank can shift the risk for a fraud loss to a commercial customer if the bank has taken three steps. Those steps, Mitchell explains, include: The bank and customer entered an agreement on security procedures, those security procedures are commercially reasonable and the bank acted in good faith in following the security procedures that it agreed upon with its customer.

Mitchell argues that the first provision, calling for a security agreement between the bank and the commercial customer, should be dropped, because it's no longer feasible in the era of online and mobile banking.

When Article 4A was written, it was relatively easy for a bank to enter a security agreement with a bank because it pertained only to wire transfers, the attorney contends. In today's much more complex environment, banks typically give their commercial customers a lengthy form that describes security procedures in general terms, Mitchell argues. And the customer generally doesn't review that document, much less discuss it with the bank, he contends.

"So the concept that the parties are making an informed agreement about what security procedures are going to be used ... simply doesn't pertain. I don't think it's realistic to think that the parties are going to sit down and talk about this," the attorney says. And many banks may not want to spell out in a document the specific security measures they are taking because the details could get into the hands of fraudsters "who might use that information in a negative way," he says.

"I think it is unrealistic, given the sophistication of [the fraud] that is happening out there today, to think that the average commercial customer is going to have any real appreciation of the threats and about how to deal with them. They're just not sophisticated enough."

Change Expectations

Commercial customers shouldn't be expected to participate in the development of a security agreement with a bank, Mitchell argues.

"The main fix is to do away with this artificial notion that the bank and the customer at the front-end ... sit down and come to some kind of agreement as to what the security procedures are," he says.

Instead, he argues, Article 4A should primarily deal with the need for banks to have a set of commercially reasonable security procedures that they carry out in good faith.

Mitchell contends that Article 4A doesn't need to contain more details on how to define commercially reasonable security. He says the term already encompasses using security measures that address the desires of the customer expressed to the bank, the circumstances of the customer and "what other banks are doing in similar situations."

In the interview, Mitchell:

- Outlines all the provisions of Article 4A;
- Describes in detail the changes he believes are necessary;
- Describes the process for changing the Uniform Commercial Code.

Mitchell recently participated in a panel discussion on account takeover trends at ISMG's Fraud Summit. A video of the panel is available on ISMG's Fraud Summit page.

Mitchell works on litigation and business law at the Maine-based firm Bernstein Shur. He's also a member of the firm's data security team, where his work in the PATCO case is noted for breaking new ground in the way courts evaluate banks' security measures.

Article 4A

HOWARD ANDERSON: So the Uniform Commercial Code has been adopted in all the states, and Article 4A deals with defining how banks need to offer reasonable security to their commercial customers. I understand that you believe courts are all over the board in terms of how they apply the statute, which you view as out date. So, first, give us a quick refresher course. Describe for us very briefly what 4A has to say about the security responsibilities of banks and their commercial customers.

DAN MITCHELL: Article 4A was drafted back in the late 1980s, and it was an attempt to try to allocate risk between banks and customers when there was an electronic fraud. Bearing in mind, back in the late 1980s, they primarily were looking at people wiring money - relatively sophisticated customers wired money. There was not a consistent, uniform approach under the law in terms of how to allocate responsibility if there was a loss for an unauthorized wire,

and the Uniform Commercial Code was an attempt to come up with a uniform way of dealing with those situations. The Uniform Commercial Code is composed of different sections that are promulgated by a national organization.

Article 4A, which … basically says if there is a fraud loss because someone who is unauthorized accesses a commercial customer's account, in the first instance, a bank is responsible for that. But the bank has an opportunity to shift the risk of loss back to the customer if a couple of things have happened. First of all, the bank and customer have to have agreed that the bank will authenticate users using a set of security procedures. So theoretically, the bank and the customer need to agree on the security procedures and what they will be. Secondly, those security procedures must be commercially reasonable as that term is understood under the law. Third, the bank needs to demonstrate that it acted in good faith and followed the security procedures that it agreed upon with its customer.

And that is basically how it works. If the bank can demonstrate those things, it shifts the risk of loss back to the customer even if the transaction, in fact, was not authorized by the customer.

Time for an Update?

ANDERSON: OK, so why do we need to change that? Is it out of date? What specific changes would you like to see?

MITCHELL: We're talking about a statute that was enacted in the late 1980s at a time when the Internet itself was in its infancy. And certainly, it is fair to say that the drafters back then had no idea what the world would like look in 2013, and they had no idea how prevalent online financial transactions would become, and they had no idea that I would sit here with my iPhone and go into my bank account and perform transactions and transfer money and do all kinds of things. So I think, just on that basis alone, it makes sense to go back and look at the statute and say, "Are these principles that we've put in place still effective today? Do they still work?"

And look, just because something is dated in the law doesn't necessarily mean it's a bad concept. … There are plenty of old concepts in the law that we apply just fine. What I'm saying is … a statute that was enacted primarily to deal with a wire transfer situation - and the standards that would have made since in 1989 - results in some problems.

For example, one of the prerequisites in the statute to a bank shifting the risk of loss is that it agreed with its customer upon a set of security procedures. That may have been realistic at one time. Maybe a commercial customer who was relatively sophisticated and did wire transfers went into your bank and talked to your account manager, and the account manager maybe brought in the operations person that said, "OK, well here are the security procedures we think make sense. If you want to do these wire transfers this is what you ought to do." And [the customer] then … said OK.

That's not what happens today. The typical commercial customer, they go to their bank, and their bank gives them a form or more likely several forms with a lot of verbiage in them. It's like reading an insurance policy - no one reads them. And maybe those forms describe what

the security procedures are, maybe they don't or maybe they just describe them generally. Very rarely have I ever seen them described specifically.

And so the concept right up front that the parties are making an informed agreement about what security procedures are going to be used, which is an important prerequisite to the way this statute operates - I think it simply doesn't pertain. I don't think it is realistic to think that parties are going to sit down and talk about this. And from the bank's perspective on things, they may not want to talk about it. I mean there may be some things that they don't want to put in an agreement - the security procedures ... exactly what they do and how they do it. That might be a road map to fraudsters who might use that information in a negative way.

So my point is, ... we ought step back and say, "Should we have a requirement in the first instance that the parties sit down and agree on a set of security procedures?" If so, then banks and customers both need to be doing more. ... And secondly, ... I think it is unrealistic, given the sophistication of what is happening out there today, to think that the average commercial customer is going to have any real appreciation of the threats and about how to deal with them. They're just not sophisticated enough. ...

I represented PATCO Construction in [a fraud] case. PATCO Construction was, by national standards, a very small company. ... They didn't have a full-time IT person. They were in the construction business. I mean, what do they know about these kinds of threats? To think that they are going to sit down in an informed way to look at security procedures and decide whether they work for them with respect to the things that are going on out there in the world today is, I think, unrealistic. The average customer just isn't that sophisticated.

So we ought to step back and look at whether we think it makes sense to have a regime that requires an agreement between bank and customer about security procedures and how much responsibility we place on the customer to participate in that decision.

Changes in Details

ANDERSON: So how much more detailed does Article 4A need to be to do the job better in the modern world, do you think?

MITCHELL: Well the problem is it's impossible to write a statute that accounts for everything that is going to happen. And I'm not suggesting that is what needs to happen. I'm not suggesting that the statute just needs to be expanded to try to look at every possible thing that could happen and account for it. If we looked at today's threat landscape and what is going on in the commercial world, we could come up with some specific areas where maybe the statute could get more specific in terms of particular types of activity and the way it should be approached.

But I'm not suggesting that is as important as just re-evaluating this fundamental question of whether there needs to be an agreement in place between the customer and the bank as to the specific types of security procedures that are going to get used and requiring a customer to participate in that discussion, essentially. Maybe one way to do it would be to simply say, "Look we're not going to require that ... there be such an agreement. We'll allow the bank to shift the risk of loss if it can demonstrate that it's got commercially reasonable security procedures, and that it has provided some level of information to their customer about what

those are. Not necessarily an agreement, because in legal parlance, an agreement is an important thing and that is different than simply a bank informing and providing information to a customer.

Defining Commercially Reasonable Security

ANDERSON: Should the code to do more to define what is commercially reasonable security?

MITCHELL: What the code does now is not bad in that area. It says primarily that a bank needs to look at what its customer is doing, look at the types of transactions it engages in, look at what other similarly situated banks are doing, look at any specific preferences that have been expressed by the customer. And so, I wouldn't say that I see a lot of deficiencies there, necessarily. And again, in our legal system there are plenty of concepts that we express generally as a starting proposition in the law and then they get fleshed out more specifically by courts in specific situations. And I don't think that is problematic. So in the short answer to your question, I would lean toward saying no, it's probably not necessary that the court get much more specific about what is commercially reasonable, because that is going to change in different situations.

Omit Agreement

ANDERSON: So what's the main fix, just to summarize, that you would like to see?

MITCHELL: For my purposes, the main fix is to do away with this artificial notion that the bank and the customer ... sit down and come to some kind of an agreement as to what the security procedures are.

The reason why there is a difference between the way we treat commercial customers and the way we treat consumers is because - and this is not just in this area in the law, but in other areas of the law - there is a supposition in the law that commercial customers are more sophisticated. They are more able to protect themselves, and consumers are less sophisticated and they need more protection. And that is a primary basis for the distinction between commercial customers and consumer customers. The notion, though, today that a small mom-and-pop commercial customer - or even a larger commercial customer for that matter - is going to understand the threats that are out there and be able to, in an informed way, participate in structuring the security procedures that are going to be in their account, I don't think is realistic.

So I would say ... perhaps do away with the requirement that there needs to be an agreement. Do away with the implicit requirement that the customer participates in deciding what those procedures are going to be. Instead, have a system in which the bank has to have a set of commercially reasonable security procedures. It should take into account the same factors - the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, what other banks are doing in similar situations. And [also include] a requirement perhaps that the bank inform the customer. Not that the bank and the customer have an agreement - but that the bank inform the customer of what is going on. If the customer is not comfortable with it, the customer can still do their banking somewhere else.

But put the primary burden in the first instance on the bank to provide commercially reasonable security procedures, which is really where it belongs. And frankly, the banks are in much better position to know what those are. Do away with this exercise that we go through in these cases where you're looking at, well, did the bank and the customer have an agreement upfront about the use of particular security procedures? Did they follow the agreement? It's a fiction that maybe in 1989 made some sense because people really did it, but in 2013, with the online banking environment, it doesn't make sense.

Changing the UCC

ANDERSON: Then real quickly, summarize for us how the Uniform Commercial Code gets changed? What is the procedure?

MITCHELL: The promulgators of the Uniform Commercial Code, the Uniform Law Commission and the American Law Reporter, who do this basically are legal professionals, professors, folks from around the country who are expert in different areas, and they meet every few years. I don't know how often the Article 4A people meet or have met to discuss proposed changes. If there is enough momentum to make a change, they'll have a meeting and they will actually issue some proposed changes. What happens with those simply is those become available to the states to either enact or not enact as they choose.

And by the way, any state can change its law any time it wants to. The theory behind the Uniform Commercial Code, though, is that we want to maintain as much uniformity as possible among the states in particular areas of the commercial law because it makes it easier for people to do business from state and state - and obviously, nowadays, that is what we do. We do interstate business. But [in] any state ... the legislature tomorrow could take up a bill and say, "We think that agreement requirement doesn't make sense we're going to take that out." But typically is not the way it works. Typically, states are reactive in this area. They will wait for the Uniform Laws Commission to promulgate a set of changes and then usually there is a period of several years of debate about whether they ought to implement the changes, whether they make sense. It is a slow process. I could not tell you as I sit here right now, based on any personal knowledge, whether there has been any discussion about changing it, what activities have taken place. I don't think there has been any. I know there haven't formally been any revisions proposed. I don't know if there has been any higher level discussion about changing it, but that it is a slow process. It would take several years.

Dan Mitchell, shareholder, is a member of Bernstein Shur's Business Law Practice Group and co-chair of the firm's Data Security Team. He can be reached at 207 228-7202 or dmitchell@bernsteinshur.com.