Bauerle's Bank Notes

November 5, 2013

"Press, Star, Pin"

"She said all you needed was a person's mobile phone number and a factory pin and you could listen to their voicemail, and actually gave an example of a story involving Sir Paul McCartney and Heather Mills," Mr Edis told the jury. --The Telegraph, Oct. 31, 2013

The NSA does it. The News of the World did it. And, according to the Germans, "the French are the worst. "[1] Electronic espionage has recently captured headlines worldwide. The NSA's surveillance program has sparked consternation, as much among Google and its peers for the revelation that their networks are porous, as among foreign governments worried about compromised state secrets. In England, eight people are on trial in the Old Bailey for hacking phones of cabinet ministers, celebrities and ordinary citizens. Consequently, businesses and governments contemplate creating national data centers in an effort to ring-fence critical IT infrastructure and data.

Banks may be tempted to yawn and say, "Welcome to my world." Since the run-up to Y2K, the industry has been bombarded with more requirements to implement IT security than any industry save perhaps the military and its contractors. Yet the proliferation of news accounts of IT security breaches and public awareness of them present new challenges to the banking industry.

Industry leaders are in the midst of converting their business model to an Internet-based exchange with customers, both corporate and consumer. Watch any NFL game this fall and you will be greeted by advertisements from Bank of America, Wells Fargo and others touting the ease of doing business with them by smartphone or tablet computer. Regional banks too are getting in on the act. A banker at a sub-$1 billion institution told me of his encounter with a friend who paid for gasoline using a debit card issued by a competitor's bank. When asked why he banked with the competitor, the friend said, "Because they

have Internet banking and I can use my smartphone." To which the banker from the sub-$1 billion bank responded, "So do we!"

Novelty and convenience are the twin draws of Internet banking. Who does not want to be in on the latest big thing? Pay or get paid anywhere, anytime, while avoiding customer lines and intrusive questions about your bona fides—what is not to like? Plenty, it turns out. For if "press, star, pin" is all it takes to access your account, as testified the £100,000/year spook hired by the News of the World to hack computer accounts of the tabloid's targets, the bad guys can steal your money just as easily. That is the dirty, not-so-little secret of the Internet economy. And it's something the banking industry must deal with preemptively.

In their contracts with customers who choose to bank over the Internet, providers like Bank of America do address, and allocate, the risks of errors and security breaches. The legal framework they have constructed is, on the whole, a reasonable one based on established and well understood concepts from the pre-Internet era. Uniform Commercial Code terms like "commercially reasonable" predominate, time periods for identifying errors match those found in the UCC governing bank drafts, and daily limits are established for the number and aggregate value of transactions, just as banks have done for 40 years for electronic funds transfers under Regulation E. The pitfalls that await the careless are described in plain English. Thus we have the following explanation of who loses when the customer mistypes the intended recipient's account information:

> You acknowledge and agree that payment transfers will be completed using only the email address or mobile phone number you enter even if it identifies a person different from your intended recipient. The name you enter will help you identify your intended recipient in the drop down menu and your transaction history but will not be used to process payments. Please make sure you accurately enter the recipient's email address or mobile phone number since your obligation to pay for the transfer will not be excused by an error in the information you enter.

The pregnant question, however, is do consumers read the disclosures lawyers write? And do they understand them if they read them? In our view, it would better serve Bank of America's purpose if the written disclosure were accompanied by an Internet tutorial in the manner of those that are routinely incorporated into video games sold over the Internet. Like driver education movies showing automobile accidents or anti-smoking campaigns featuring pictures of smoke-damaged lungs, tutorials are needed that show consumers waving goodbye to their money as it wings its way over the Internet to Mumbai as a result of the sender's miscoding the receiving bank's routing number or the intended recipient's account number. Otherwise, it is only a matter of time before the plaintiffs' bar cooks up lawsuits that blame banks for consumers' losses despite the unmistakable disclosure quoted above.

At the dawn of the Internet era, I met a retired Air Force colonel then working on the earliest efforts to construct an antiballistic missile shield. After hearing me explain my work with banks and bankers he said, "We're both in the same business." I gave a puzzled expression. "We both work with complex adaptive systems," he added. Internet banking is indeed a new layer of complexity added to an already complex adaptive system. The challenge we face is to make the system serve its intended purposes well, with few and minor errors and breakdowns, while protecting it and its users against those who would manipulate it to serve their own corrupt purposes.

[1] "NSA Claims Put German Businesses on Guard," New York Times, Nov. 1, 2013. The French meanwhile joke that Americans' eavesdropping on the French government offers no advantage, due to the high level of dysfunction that pervades the French government. See Financial Times, Nov. 2, 2013.