Testimony of James R. Woodhill
Advocate, Government and Public Relations
YourMoneyIsNotSafeInTheBank.org
Before the U.S. House of Representatives
Committee on Financial Services
Subcommittee on Capital Markets and Government Sponsored Enterprises

June 1, 2012

Chairman Garrett, Ranking Member Waters, and members of the Subcommittee, thank you for the opportunity to testify today on behalf of the current and future victims of commercial-account account takeover fraud.

My name is Jim Woodhill. In December of 2009, I was recruited by Avivah Litan of Gartner, Inc., the leading industry cybersecurity analyst, to bring this crime to the attention of the Congress. Ms. Litan knew me as the founder, a decade earlier, of Authentify, Inc., one of the now scores of security solution providers with offerings that address this specific crime. I am now the government and public relations advocate for YourMoneyIsNotSafeInTheBank.org.

I am appearing before you today because your money is not safe in the bank. At least it is not if you are an American church, school district, public library, or small business that banks online on a Microsoft Windows PC. Shockingly, as is an official banking industry policy the American Bankers Association (ABA) calls "shared responsibility"— should foreign cybercrooks' malware takes over your PC and then that PC tells your bank's Internet banking system to transfer all your organization's money to Romania, you are out the money stolen in that cyberattack.

This doctrine of "shared responsibility" is bankrupt as security policy and is politically illegitimate. It is also heroically bad public policy because the money being stolen is funding rapid advances in cyber-attack technology, and we are starting to see crossover between cybercrime and cyberattacks by nation state actors. What was a smallish crime of fraud two and a half years ago is now part of a full-blown national security crisis, which extends beyond financial services. For these reasons alone it is not enough to rely upon our country's diverse population of commercial online bank account holders to keep pace with this evolving threat. On October 7, 2009, even FBI Director Robert Mueller mentioned in a speech in San Francisco that he had stopped banking online because he did not believe *he* could do so securely. If we are to turn the corner, these crimes must be stopped by utilizing combinations of technologies that have existed for years.

The first known victim of this crime, a family printing-cartridge business in Miami, lost $90,000 in April of 2004. It was not the crime, but Bank of America's unwillingness to make good on the loss that ignited a media firestorm so intense, The New York Times was still running articles about the case eight months after the news broke.

The Lopez family filed suit against Bank of America in February of 2005. Thereafter, the bank finally compensated the Lopez family for their losses, nearly two years after the crime had occurred. By then, the regulators had already reacted to this crime. In October of 2005, the Federal Financial Institutions Examinations Council (FFIEC) issued guidance entitled "Authentication in an Internet Banking Environment", describing the crime of malware-based account takeover and instructing the F.I.s under its purview not just to adopt the fraud controls needed to prevent the crime, but to keep those controls

updated as the cyber-threat landscape evolves. No more cases surfaced in the news in the next couple of years.

By late 2008, the criminals re-emerged with "ZeuS", a new generation of malware that was much more powerful, persistent, and could be wielded by a criminal with no technical background. Within a year Ms. Litan was so alarmed by the mounting losses and the banks' lack of response to them that she put me in touch with Brian Krebs of the Washington Post, who was, and still is, the lead reporter on the cybercrime beat. Mr. Krebs directed me to the Post's archive[1] of his stories about victims and put me in contact with a number of them. However, since our group launched http://www.yourmoneyisnotsafeinthebank.org[2], new victims have started approaching us directly.

One of the latest victims of this scheme to contact me is TRC Operating Company, Inc. of Taft, California, an independent domestic energy producer, which has since filed suit over its victimization by the ironically-named United Security Bank of Fresno just two weeks ago. Eastern European cyber-criminals attempted to siphon more than $2 million out of the company bank account.

The stories all sound the same. A small- and medium-sized enterprise that banks online at an American small- and medium-sized bank somehow ends up with malware on the Windows PC it uses for online banking. The typical transmission vector is a successful email "phishing" attack that gets an unwary user to open an infected attachment file or visit a compromised web site. However it gets on the user's PC, the "ZeuS Trojan" infiltrates the user's web browser and watches for online banking logons. If the bank's URL is one of those known to follow the "Krebs Rule", which employs fraud controls that are effective even if the user PC is totally under the control of the enemy, the malware gives up and its human master spends his time trying to infect other PCs. However, if the F.I. is one that does not follow this rule, the criminal uses his "Man-In-The-Browser" attack kit to either capture the customer's logon credentials for separate use, or to actually hijack the customer's validly authenticated online session and use it to transfer money to accounts controlled by the criminal. While all of this is happening, what the user sees on his screen gives no hint that such is going on behind the scenes.

Even today, 70% of the time such an attack is conducted, the F.I. learns of it from its customer, rather than detecting it itself. Thousands of American organizations have been the victims of online bank robbery, and over 500 have lost money that was not reimbursed by their bank. Online bank robbery became a much more lucrative crime than physical bank robbery years ago.

---

[1] Washington Post Security Fix
http://blog.washingtonpost.com/securityfix/archives.htm

[2] http://www.yourmoneyisnotsafeinthebank.org

Dismayingly, neither the FDIC nor law enforcement knows for sure how many attacks there are and how much money in total has been lost, much less the split between the victim and the bank. Many banks do the right thing and cover such losses completely, though others do only partially—just enough to keep the victim from suing. Brian Krebs believes that only a fraction of account takeover incidents are reported to law enforcement.

At its Symposium on Combating Commercial Payments Fraud[3] held by the FDIC on May 11, 2010, the word "crisis" was used by both FDIC and law-enforcement officials. Those FBI agents stated that they were investigating 250 cases at that time, and the rate of growth they were seeing in victimization was 5X every twelve months. The estimate they offered was $70 million lost by commercial victims as of that date. In Assistant Director Snow's testimony, he stated that the FBI was investigating over 400 cases of account takeover fraud involving the attempted theft of over $255 million, resulting in the actual loss of approximately $85 million.

All of the victims of this crime, which is also referred to as "account-takeover fraud" or "ACH fraud", have gone through the same stages of a special grief process:

SHOCK--that their money could be stolen electronically

DENIAL--they just can't believe the official policy of America's banking industry is "shared responsibility", which in practice means "no responsibility" for keeping their organization's deposits safe, even though federal law forces them to take full responsibility for personal accounts.

ANGER--Why didn't my bank call me? I get calls all the time about charges on my credit card! Why won't they take responsibility? They urged me to sign up for online banking, and claimed it was safe! You mean "FDIC Insured" does not mean I will get my money back either? How could my PC have gotten infected? I run Norton anti-virus and update the product four times a day!

BARGAINING--trying to cut a deal with their bank to get an acceptable percentage of money back.

The last stage of the normal human grief process is commonly termed "ACCEPTANCE". Well, there is never any "acceptance" by the victims in these cases. Instead, there have been about a dozen lawsuits by victims who still had the means even after they were robbed. However, other victims simply went bankrupt. That would have been the fate of Karen McCarthy's Little & King, had I not extended a $100,000 loan to it. It was and is a

[3] Symposium on Combating Commercial Payments Fraud. FDIC. May 11, 2010. http://www.fdic.gov/news/conferences/2010_fraud/agenda.html

great little business. It has made every payment on time, with interest. But without my help, it would have died, forcing the family it was supporting to pull its two kids out of college and lose their house. Mrs. McCarthy's husband was one of those brave New York firemen badly disabled responding to 9-11.

Since the original "Lopez" case, a number of these crimes have ignited additional media firestorms. One such case is PlainsCapital Bank vs. Hillary Machinery, Inc.[4] in early 2010, the bank filed suit against the victim of an account takeover. I have accumulated almost 5,000 news stories and technical articles on this crime, comprising almost 2 gigabytes of data. Never have I seen anyone outside of the financial services industry publicly defend the notion that banks are not responsible for keeping their depositors' money from being stolen. How can security measures and policies be "commercially reasonable", when, if the customers only knew what these policies were, the organization would have no customers? The ABA's arguments defy the common sense of average citizens, not to mention their sense of right and wrong.

It also defied the common sense of Senator Chuck Schumer, who, on September 29, 2010 introduced S. 3898[5], a partial extension of Federal Reserve Regulation E to cover state and municipal accounts.

That banks are not responsible for safeguarding their depositors' money from risks that have not even been disclosed to those depositors is a position unlikely to be sustained in the courts. Responsibility for the safety of bank deposits and the terms of the account agreement between bank and customer are governed by federal legislation and regulation, state contract law (specifically Section 4(a) of the Uniform Commercial Code (UCC)[6]).

For individual accounts, which are tied to a Social Security Number, there is no ambiguity. The Electronic Funds Transfer Act of 1978 (EFTA)[7], whose regulatory perfection is Federal Reserve Regulation E, commonly known as "Reg E", requires financial services institutions to make good on any losses, even if the user posts his

---

[4] PlainsCapital Bank vs. Hillary Machinery, Inc.
http://dockets.justia.com/docket/texas/txedce/4:2009cv00653/120329/

[5] S. 3898
http://www.govtrack.us/congress/bills/111/s3898

[6] Uniform Commercial Code Section 4(a)
http://www.uniformlaws.org/ActSummary.aspx?title=UCC%20Article%204A,%20Funds%20Transfers%20(1989)

[7] Electronic Funds Transfer Act of 1978
http://www.fdic.gov/regulations/laws/rules/6500-1350.html

online banking userid+password on Facebook. However, EFTA was explicitly a *consumer* protection act. EFTA did not say banks are *not* liable for safeguarding commercial accounts, those under a Federal Employer Identification Number. It was simply silent on the matter.

Account takeover fraud loss liability is therefore governed by the contracts between the parties. However, these contracts must conform to the Section 4A of the Uniform Commercial Code (UCC) of whatever state the contract says its law will apply. Section 4A mandates that access to funds must be safeguarded by a "security procedure", and said procedure must be "commercially reasonable".

What is and is not a "commercially reasonable security procedure" is, therefore, the central subject of all the lawsuits. However, other causes of action can, and have been brought, including the argument that under the common law, banks are responsible for keeping their depositors' money from being stolen. "Commercially reasonable" is a legal term of art whose meaning is analyzed in depth in "The Commercial Reasonableness of Bank ACH Security Procedures"[8] by Brad Maryman and Dr. Stan Stahl. It was also the subject of a mock trial at the 2011 RSA Conference entitled, "Whose Fault Was It That I Did Not Know You Were You?"[9], which was presided over by federal magistrate John M. Facciola. In that session, as in the real case of PlainsCapital Bank vs. Hillary Machinery, Inc., I was expert witness for the victim *pro bono*. Of course, I could not speak to the meaning of the legal term "commercially reasonable" in UCC-4A, as we had two top lawyers argue that. My role as a security expert was to testify that the online banking fraud controls of the bank in this hypothetical case, even if they met the test of "commercially reasonable" in some abstract legal way, had not provided what a "reasonable man" would consider "security" in the technical sense, nor did they comply with the 2005 FFIEC Guidance. Given that this was a jury trial, and the jury was the audience, the victim won easily.

In any such real lawsuit, the F.I. would be well advised to avoid a jury trial. Were I a lawyer, I would not take the case of the bank. But if I had to, I would have to challenge the seating of any juror who had any interest in a commercial bank account, or attended a church, had kids in a school, or lived in any local political entity, because organizations of all these types and more have been victimized. I would demand that any judge with

---

[8] "The Commercial Reasonableness of Bank ACH Security Procedures" http://www.citadel-information.com/wp-content/uploads/2011/04/commercial-reasonableness-of-bank-security-procedures-101207.pdf

[9] "Whose Fault Was It That I Did Not Know You Were You?" http://cornerstonesoftrust.com/presentation/whose-fault-it-i-didnt-know-it-wasnt-you-panel-discussion

such conflicts recuse themself. It is likely that there is no judge in America that would pass such a conflict-of-interest test, and perhaps no potential juror.

Right now, the official lawsuit tally is one finding for the victim and one for the bank, with three settled on terms favorable to the victims and at least seven ongoing. Besides the case brought by the Lopez family, there have been at least two other lawsuits where the bank settled immediately after hearing what the judge in its case had to say, in addition to his or her denial of the bank's motion for summary judgment. At the 2012 RSA Security conference in March, which was attended by 22,000 security professionals, there was a follow-on session to our mock trial back in 2011. At this new session, a panel of top cyberlaw experts, led by U.S. federal magistrate John Facciola, predicted that, considering that the 2011 FFIEC Guidance was now in effect, going forward, such cases would increasingly end with summary judgment for the plaintiff.

The one case that was "won" by the bank, PATCO Construction vs. People's United Bank[10], the judge had to overlook the fact that Oceans Bank, which was acquired by People's United Bank after the crime but before the lawsuit, had ignored the fraud alerts sent to the bank by its outsourcer. The outsourcer had scored the bogus transactions' risk at "800" versus at most "8" for previous transactions. You are hearing me correctly. In the PATCO case, all the technical fraud controls necessary to have saved PATCO's money were already in place and operating. Nothing new needed to be implemented or even understood. All the costs were already being billed by the processor to the bank. As I have said previously, technically, this is a long-beaten problem. I put the word "won" in quotes, because PATCO Construction's attorneys estimate that Peoples United has to date spent over $1 million in legal fees to avoid reimbursing a $360,000 loss, defending its policy of "shared responsibility".

It is precisely this type of event, yet higher profile, which could spark a mini "run on the banks". Depositors would flee from any bank without proper security measures to those banks that provide adequate protection and/or absorb any losses. As soon as anyone with an interest in a small- and medium-sized enterprise learns of the threat from malware-based account takeover and visits YourMoneyIsNotSafeInTheBank.org, they are urged to take a letter demanding liability disclosure to their bank. If the customer is not satisfied with their bank's protection, they are advised to move their accounts to a bank where they are protected. To know about this attack is to be very quickly safe from it.

To bring this point home, any member of this Subcommittee whose campaign fund banks online could see its funds vanish into eastern European bank accounts overnight. Rest assured, Mr. Chairman and Ms. Ranking Member that at the Symposium on Combating Commercial Payments Fraud conducted by the FDIC on May 11, 2010, Bryan Nash of Illinois-based McHenry Savings Bank, who led the panel of bankers who vigorously

---

[10] PATCO Construction vs. People's United Bank
http://voices.washingtonpost.com/securityfix/Complaint%20091809.pdf

defended the ABA's doctrine of "shared responsibility", replied to my specific question that if the campaign funds of a member of the House Committee on Financial Services were ever stolen, your campaign would be fully reimbursed without the Member even having to ask. The campaign treasurer involved would have some shocking and scary moments, and it might take a few days for your campaign's money to be "restored" but quite soon you would be made whole. Yet again, who's to say what the criminals are doing with their loot.

It is only the Hillary Machinerys, PATCOs, and Duanesburg School Districts that are at risk of total, or at least partial loss. Indeed, at Cherry Hills, NJ-based TD Bank, if you are the Town of Poughkeepsie, NY and you have $378,000 stolen by cyber-thieves, you will be fully reimbursed, at least after your state's senior senator introduces legislation to extend Federal Reserve Regulation E to cover municipal accounts. But if you are tiny Little & King on Long Island, banking at that very same F.I., your $120,000 loss will be allowed to bankrupt you.

I am here to argue against either the victims or small- and medium-sized banks having to bear the losses or the risk of losses itself. Note that it does not matter whose pocket the tens of millions currently flowing overseas from U.S. bank accounts comes. It's helping to fund the R&D efforts of criminal masterminds with whom a little money buys a lot of software development. That money is also funding the building out of an entire criminal economy, on which today one can buy, for example, the full identities, including Social Security Numbers of thousands of Americans over the age of 65 and then commit Medicare billing fraud, or any other species of identity theft.

Who in the world could defend the position of the ABA on account takeover, especially when the continued flow of victims' money overseas is funding the advancement of such destructive software? The lack of support among the public for the ABA's position makes it particularly ironic that I, the advocate for the victims, must speak in support of it.

On April 19, 2010, I met with Ms. Feddis and her partner Doug Johnson at ABA headquarters. They had told members of this Subcommittee, who had inquired after I met with them, that extending Regulation E to cover commercial accounts would "drive community banks out of online banking." At the end of a 2-hour meeting, I came away with the realization that they were correct. America's small- and medium-sized banks cannot take on liabilities that they lack the skill and, just as importantly, the scale to manage.

I also realized at that meeting that government affairs people, even those working for the ABA, are not necessarily well informed on the technical capabilities of the latest-generation fraud controls. They claimed that there were no purely technical solutions to this crime. That was only true if one would argue that Oceans Bank had no technical solution in place because it had not staffed the business process (examining the fraud alerts sent to them by their processor) that supports that technical solution. That's a stretch. In any case, Mr. Johnson was working his heart out to educate his membership

about ZeuS and its cousins so they could stop these attacks he simultaneously stated they were not responsible for.

My conceding the correctness of the ABA's position that America's small- and medium-sized banks cannot bear the risk of this crime does not mean I can support their doctrine of "shared responsibility". That America's small- and medium-sized banks do not have the cybersecurity solutions and skills, nor the financial scale to bear the risks and responsibilities associated with online banking (which, of course, they probably *do* have under existing law), does not mean that their small- and medium-sized enterprise customers can either. By 2008, the firewall and anti-malware products that had protected them in 2005 had been beaten by the fraudsters and remain impotent. In any case, given that hospitals cannot move the needle on getting doctors to follow hand-washing guidelines, the notion that 20+ million small organizations are going to execute cybersecurity measures flawlessly day in and day out is preposterous. There are offices within the Congress that have had to have every single Windows PC replaced twice now because they had become so deeply infected by malware that no remediation was possible.

Let me emphasize that this is not a criticism of the management teams of America's small- and medium-sized banks. It was patently obvious when I met with the ABA that in spite of the FFIEC's Guidance and even the FDIC's August, 2009 Special Alert[11], they had not heard of this crime. As I will show below with an example from gastroenterology, information moves through a profession at a pace that can only be characterized as glacial, outside of situations that no one could wish to happen.

PlainsCapital Bank vs. Hillary Machinery, Inc. was a case in point why the FFIEC had to issue its supplemental Guidance in June of last year. PlainsCapital employed "two factor" authentication, but it was a fake version that amounted just to a few additional passwords, called "challenge questions". No security expert would have mistaken challenge questions for the "second factor of authentication" called for in the 2005 Guidance. However, back then the regulators had bent over backwards to be "technology neutral" in their recommendations and some security startups took advantage of that and the banks' lack of expertise to sell them "two-factor" authentication that was really a single factor twice.

Let me also explain that those banks that were aware of this crime but did not have deep in-house cybersecurity expertise were hampered in responding by a subtle intellectual confusion that the regulators inherited from my own information security industry. The problem can be seen in the title of the October 2005 FFIEC Guidance, "Authentication in an Internet Banking Environment". Back then, session-hijacking attacks were unknown, so the focus was on preventing attackers from using malware to steal logon credentials

---

[11] FDIC Special Alert. August 2009.
http://www.fdic.gov/news/news/specialalert/2009/sa09147.html

and then use them to impersonate the victim from their own PCs. This kind of attack was what was used to steal, in early November of 2009, over $800,000 from the accounts of Plano-based Hillary Machinery, Inc. at Dallas-based PlainsCapital Bank (PlainsCapital managed to claw back $600,000 of that sum). Note that this is the infamous case where the bank sued the victim, in spite of PlainsCapital's CEO having received the FDIC's Special Alert on August 26 of that year and also, in spite of being out of compliance with at least the spirit of the 2005 Guidance, because PlainsCapital's "two-factor" authentication technique was based solely on "Things You Know" that could be stolen in a single malware-based attack and used elsewhere.

At the 2010 FDIC Symposium, I spoke with a number of community bankers, including Bryan Nash of McHenry Savings Bank. They were all earnest, salt-of-the-earth people who would not buy into a doctrine as commercially and politically toxic as the ABA's "shared responsibility" (for account takeover fraud) if they weren't being squeezed by forces they could not manage. I think it is very important to note that ZeuS emerged at about the time Lehman Brothers' collapse plunged the entire world economy--via its banking system--into a crisis that lingers to this day. Community Bankers were hit with huge new FDIC assessments to bail out a small number of their foolish (or worse) lenders to the residential real estate market, not to mention having the mountain of financial industry regulations they have to comply with greatly grow in height. They had a lot more on their plate than remote-sounding cybersecurity threats.

The specific fear bankers articulated privately is that if they signed up for their processors' advanced fraud controls, the small- and medium-sized enterprises that bank with them would just "take their business down the road to a competitor that does not impose such hassles on them." As a security guy, I was baffled by this statement, and had to struggle to understand the world from the point of view of the CIO of a community bank. However, at the FDIC Symposium, Murray Walton, Chief Information Security Officer (CISO) of Fiserv, one of the largest processors told the audience that he must have pitched "two dozen" bankers on his company's advanced fraud controls, and made no sales because the bankers had never heard of the problem and/or did not believe it could happen to them. All of them subsequently had victims. His processor had the needed solutions, but it could not force customers to adopt them.

The deep intellectual problem that community bankers had inherited from the security community via the FFIEC Guidance was that the answer to account takeover / ACH Fraud was better online banking user authentication at logon. The very name of the FFIEC Guidance embodies that subtle flaw in thinking. And yes, it's a tremendous hassle for people to have to have an RSA SecurID on their keychain and to use it every time they log on even just to see if a check cleared. Mr. Nash and his fellows assumed that I was now also asking them to demand that their SME customers go through an extended "transaction confirmation" process for every online payment they do.

I realized that "transaction confirmation" was the term of art that had to replace "user authentication" in the conversation about account takeover. But the only transactions that had to be confirmed were "ADD PAYEE" and change-of-account-control information

(e.g., the contact phone number on an account). These are very, very rare transactions for the typical online banking customer, yet criminals cannot make off with a customer's money by paying its phone bill excessively. All the crimes involve adding new payees overseas, or at least adding domestic U.S. "money mules" to the organization's payroll and then giving them incredibly large hiring bonuses. None of the crimes have been at all subtle. At Choice Escrow of Springfield, Missouri, BankCorp South allowed the entire contents one of its title accounts to be transferred to a new payee on the island of Cyprus on March 17, 2010, it helpfully loaned the victim $90,000 so the overdraft the cyber-bank-robbers had created would not prevent the transfer from happening. Choice has sued. BankCorp South, another F.I. that used one-factor security twice and calls it two-factor, has replied to the suit that their online banking security measures were completely adequate, and, anyway, they have abruptly and massively upgraded them! Again, I cannot speak to "commercially reasonable". I have come to talk to you about "security" and how the victims our little organization represents did not have the benefit of it at their banks.

Ironically, the regulators know that the key transaction that requires many-layered defense is "ADD PAYEE", they were just not clear about that in their 2011 Guidance[12]. Studies by Javelin Research of customer acceptance of having to take the occasional call to verify, for example, that Duanesburg School District really did intend to add twelve new payees in Russia and the Ukraine over a long holiday weekend, increase customer satisfaction, not decrease it. These findings were presented at the FDIC Symposium, but the speaker and the regulators were thinking of single-digit numbers of ADD PAYEEs a year, while the bankers were thinking in terms of the hundreds or perhaps even thousands of logons and payments they did. The latter is literally three orders of magnitude greater than the former, and would indeed represent imposing an unbearable amount of security hassle upon online banking customers.

If the FFIEC had issued Guidance on how to stop account takeover five years earlier and the technical solutions were easy and cheap, then how can I say that the banks can't be held responsible? Here, I am making a "public policy" argument not a legal one. At a conference at Brown University that I attended just last month, one of the most cybersecurity-savvy members of the House, Congressman Jim Langevin, went out of his way to observe that America needs 20 to 30 thousand fully-technically-qualified "cyberwarriors". He then stated that we have perhaps 1,000 today. When the FFIEC Guidance was issued, we had a small fraction of that and quite a few more F.I.s than we have today. America's community bankers are not cyberwarriors, nor can they hire cyberwarriors. It's one field in which the unemployment rate is zero.

Security experts could cite your (or the ABA's) chapter and verse about how account takeover was a beaten problem, technically, back in October of 2005 when the regulators first issued Guidance warning of this problem and advising America's F.I.s on how to

---

[12] FFIEC 2011 Guidance.
http://www.ffiec.gov/press/pr062811.htm

keep it from happening. Faithful adherence to that original Guidance by one as skilled in the art of cybersecurity as one of Rep. Langevin's 1,000 cyberwarriors, using the security solutions available back then, would have thwarted 100% of the attacks whose details have been made public to date. Today's security solutions are inexpensive, quickly implemented, cheap to run, and enjoy high customer acceptance. If the "layered security" called for in the 2005 FFIEC's Guidance is implemented using information security best practices, the current solutions are more than sufficient. The root cause of crime is "criminals", and criminals are not like nation states. They are profit-motivated. While they will never go straight, they will switch to some other crime once stealing $1 starts costing $10.

The next attack is always right around the corner. Organizations big enough and smart enough can always withstand the attacks and protect their customers. But such organizations will always be few in number compared to the total size of the membership of the ABA. Over time, small organizations could gain in cybersecurity expertise, but over that same period of time the attack landscape will grow as much or even more complex.

Should that little northeastern bank have already been moving? On August 26, of 2009, the CEO of every FDIC-insured institution received a one page Special Alert from the FDIC specifically warning about the epidemic of account takeovers and warning them to take appropriate measures to safeguard their customers' funds. Yet, the following April, I spoke with the CIO of a tiny (just 200 commercial accounts) community bank on whose board he then sat. The CIO had never heard of the attacks mentioned in the 2005 Guidance or the 2009 Special Alert either. Despite the efforts to educate him by the FDIC and also his current outsourcer, who had the necessary security measures in his current online banking platform, my description of the attacks and recommendations on how to stop them were completely new news.

Was this CIO incompetent? Not a bit. I know talent when I talk to it, and also commitment. Cybersecurity is just too big and complex for small organizations to deal with.

That we have no hope at all of meeting the threat of account takeover by educating community bankers to be cybersecurity experts is nowhere more easily visible than in medicine.

On September 28, of 2006, the Centers for Disease Control published a bulletin on its web site that said, "Good News - A Cure For Ulcers!!"[13] This news item breathlessly announced that:

---

[13] "Good News – A Cure For Ulcers!!" Centers for Disease Control. September 28, 2006 http://www.cdc.gov/ulcer/consumer.htm

> Recently, scientists have found that most ulcers are caused by an infection. With appropriate antibiotic treatment, your ulcer - and the pain it causes - can be gone forever!

A little digging finds that "recently" meant that two Australians had won the Nobel Prize in Medicine a year earlier for this discovery that they made in 1981 and about which the paper that won them the Nobel was published in 1985. Note that the number of gastroenterologists in America is about the size of the membership of the Independent Community Bankers of America (ICBA). Unlike the bankers, however, treating peptic ulcers is a gastroenterologist's core business. They are under a continuing medical education mandate to keep their licenses. Still, 20 years is the typical amount of time it takes to ripple a change in the standard of care through a medical specialty, even when the stakes are life or death. I will circle back to medicine because it offers the one acceptable model I have been able to find for how the learning curve of a professional specialty can be accelerated.

Again, I was founder and chairman of a company that had one of the solutions, yet a paper had been published by the University of Mannheim (Germany) a year before I was contacted about the crime wave, which analyzed the emerging ZeuS malware-based attack kits. While I was just on the board of a solution provider, information security was my field. I had a 40-year career in enterprise software with the last 15 focused on information security. Can we ask a Duanesburg School District or a Hillary Machinery, Inc. to do better than I did? We cannot even ask this of a McHenry Savings Bank. Members of the subcommittee: a number of you heard about this crime for the first time from me in early- to mid-2010, yet two of you had victims in your district after this time.

I see public health's experience with using education and awareness for infection control repeating in our experience with the Conficker worm, which was first identified in November of 2008. The count of infected PCs is once again on the rise after being beaten back for a time by the Conficker Working Group and updated antimalware solutions. Conficker propagates by exploiting weak passwords on administrator accounts. Efforts to educate users to employ strong passwords predate the widespread commercial use of the Internet itself. If "education" and "awareness" efforts could accomplish anything at all with end users, there would be no weak passwords out there to be exploited. Alas, there are millions and millions of them on devices as varied as PCs, servers, and routers.

The 112th Congress' work on cybersecurity is encouraging. In the House's First Session, the cybersecurity task force, led by Congressman Mac Thornberry, led the way by synthesizing the best thought and opinion from the public and private sectors to lay out a roadmap for thoughtful legislative action. But in 35 hearings in the House alone, experts from both the public and private sector, while specific about the threats and the magnitude of the dangers, have been vague about solutions. I will be specific about the solutions I recommend to beat account takeover, but they will not work well in isolation.

I believe that they will be most effective if implemented as part of a comprehensive national cybersecurity strategy.

On November 22 of 2011, the Administration released its Comprehensive National Cybersecurity Initiative[14] (CNCI) which laid out three goals--establish a front line of defense against today's immediate threats, defend against the full spectrum of threats, and strengthen the future cybersecurity environment--and 12 separate initiatives to further these three goals. I tried to fit my proposal into this strategic framework.

In my view, to make cyberspace a "safe neighborhood", a comprehensive cybersecurity strategy for the U.S. would have four elements:

1) Harden American IT assets against cyberattack. The single most important thing we need to do is find a way of getting Norton (Symantec) and McAfee anti-virus products actually protecting again, along with the products of their 29 competitors. I have a specific proposal to accomplish this that I have been trying to interest the incumbent vendors in.

2) Make the work of cyberdefenders and fraud-fighters easier. Chairman Mike Rogers' Cyber Intelligence Sharing and Protection Act (CISPA) is an important step in this direction, but there are many more I could propose.

3) Determine the best use of government resources, especially those of law enforcement, in accomplishing the above two goals. The way many victims of account takeover have learned that they were being robbed is that they got a call from Washington Post reporter Brian Krebs, warning them that at that very moment, the cyber-crime was in progress. Brian somehow learns of these crimes in real time by monitoring ICQ (an Internet protocol used for chatting) traffic, yet this is much more useful and leveraged work than spending years trying to slap handcuffs on some kingpin in Ukraine.

4) Implement a decisive solution to the problem of "identity". The intersection of "identity" and "public policy" is the most intractable part of cybersecurity because we have not solved it in physical space, so there is nothing in place to be extended into cyberspace. I sketched out a solution, in response to the Financial Services Committee's hearings on FACTA and identity theft, which I came to call the Personal Identity Control System (PICS). Unfortunately, even though the PICS is simple at its core, defining its edges is much more difficult. However, we won't be secure in physical space, much less cyberspace, until we have something like the PICS.

---

[14] "Comprehensive National Cybersecurity Initiative" http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

It may sound strange that America needs to articulate "we must stop our churches, school districts, and small businesses from being robbed" as part of a new cybersecurity strategy, but I am offering this testimony because this has not yet been accomplished. Achieving this will, as I expand upon below, require moving the risks and responsibilities associated with operating in cyberspace to the entities most able to bear and mitigate those risks. It will also require, however, making the jobs of American cyberdefenders much easier and the jobs of foreign cyberattackers much harder, hence my brief mention of needing an overall strategy for security in cyberspace.

Let me now speak specifically to stopping malware-based account takeover attacks by a date, if not by the end of this year, certainly by the end of next.

While there are a lot of people involved with cybercrime, at the core there are a small number of hacker geniuses in Eastern Europe, China, and elsewhere, on whose innovations the entire criminal and nation-state cyberattack ecosystems depend. Any effective strategy for making cyberspace a safe neighborhood will require a larger, but still relatively small, number of cyber-geniuses on our side to defend all our IT assets. In the words of Rep. Thornberry and also Senator McCain, we need "active defenses" in cyberspace.

Community banks are not just an important part of the American economy; they are an important part of American society. They are small enough to actually know their customers, and make a living out of making loans to productive enterprises, rather than having to rely on a few large banks. Their management must spend all of its time thinking about expanding its financial assets (loans), not defending its cyber-assets.

Let me specifically speak to extending Regulation E to commercial accounts. My meeting with the ABA convinced me to oppose that solution. This does not mean I am not appalled by the doctrine of "shared responsibility" they attempt to defend. It does not make even commercial sense. In a free-enterprise system, companies like the ones I started got paid for taking on customers' responsibilities and discharging them better/faster/cheaper than our customers could do themselves.

Fortunately, the typical F.I. that is too small to do cybersecurity is also too small to actually run its own online banking information technology. At least 5,000 American small- and medium-sized banks outsource online banking to one of only 13 online banking platform vendors, or "processors". All of these organizations have the characteristics of an organization to which the risk of account takeover and the responsibility to stop it can be transferred:

- They run the IT on which online banking is actually conducted, so they are positioned to install and use the security solutions that have already been proven in the field as able to stop this crime. Indeed, some of them, at least on some of their online banking platforms (many processors have more than one), have already implemented the necessary layers of security solutions that have been proven in the field to defeat

commercial-account online banking funds transfer fraud, and they have been trying to get their customers to adopt those solutions for years now.

- They are small enough in number that they can acquire the necessary expertise to understand the cyber-threat landscape they face and track its evolution.

- They have sufficient capital to take a few losses, and they host enough large accounts to attract the attention of giant insurers who are already in the cyber-loss business, should they feel they need to lay off some of the risk, rather than being self-insuring.

- They are large enough to hire staffs to do forensics on novel attacks.

- They can establish and maintain working relationships with national law enforcement agencies such as the U.S. Secret Service and the FBI, who have the jurisdiction and resources to pursue the criminals behind attacks.

- They stand to profit from protecting their banking customers and their account holders. Commercial-account online banking funds transfer fraud losses are much greater than the cost of the security solutions, so it offers the processors the opportunity to profit at the cyber-criminal's expense. Indeed, many of the processors are already trying to get their customer banks to buy advanced security solutions from them, but the customers just don't understand the threat. Right now, the fraud losses are higher than the fraud control costs needed to stop them, so this is an opportunity for money currently ending up in the pockets of the criminals to find its way to the bottom lines of the processors.

- They stand to lose from *not* protecting their small- and medium-sized bank customers' online banking customers, because if commercial-account online banking funds transfer fraud is not stopped, the word would eventually get around that small- and medium-sized enterprises' money is not safe in the banks who are the processors' customer base, and those SMEs would move their accounts to large banks who run their own online-banking IT and who put their money where their fraud controls are.

- They all compete for customers across our entire nation. This reform will enable them to start competing on the basis of cybersecurity effectiveness, fraud control cost, and minimum end-customer security hassle along with today's competitive factors.

The processors own the server side of online banking, where the overall business processes by which funds are transferred can be protected against attack. As Congress has heard from witness after witness in hearing after hearing in the last two years, there are no reliable user-client-side solutions. While "good cyber-hygiene" might stop 85% of individual attacks, as documented in Rep. Thornberry's task force report, the bad guys have unlimited "at-bats" with no "called-strikes". The way they work is to try the oldest and simplest attacks first, while resorting to valuable "zero-day" (previously unknown) Windows exploits only when easier/cheaper attacks fail and the target is valuable enough. A relatively small number of them can force us to try to defend tens of millions of attack

points. Stopping 85% of the attacks will not protect 85% of the targets. The bad guys keep escalating.

All the client-side anti-virus solutions were beaten years ago. All the victims I spoke with had firewalls in place and they were running anti-malware solutions with up-to-date signature. It did not save them from ZeuS. All such products are now part of the test suites for the malware makers, and they keep working until their new version defeats them all. The individual small- and medium-sized enterprises are helpless before attacks by which even the laboratories that design America's nuclear weapons have been penetrated.

On April 21 of 2011, Gartner release a research report entitled "The Five Layers of Fraud Prevention and Using Them to Beat Malware"[15]. Those in charge of running online banking IT need only get a copy and line up its recommendations with the enhanced Guidance the FFIEC released on June 28, 2011 plus its original 2005 Guidance.

A useful goal of this effort is to bring the losses to account takeover down to zero without future Little & Kings or McHenry Savings Banks having to even know that there is (or rather "was") such a crime.

I have nothing against user awareness. I like the idea of an informed citizenry. I just insist, as the designated advocate for the victims and de facto advocate for our small banks, that they all get to live in a safe cyber-neighborhood. I lent Karen McCarthy's company $100,000 to keep it from going bankrupt when TD Bank let cybercriminals make off with that much of Little & King's money. But before I transferred the funds, I made sure that she switched to banking in the same place I have always had my own commercial accounts, an institution that requests to remain nameless. I have made the same demand of any other entity to whom I have extended loans.

Why would a bank that has invested in industry-leading technical controls and fraud control expertise not want its name mentioned? It's the reason that no U.S. bank competes on keeping SMEs' money safe in the bank. They don't refer to the eastern European criminals as being "the Russian mafia" for nothing. The web sites of more than one U.S. money-center bank have been knocked offline by DDoS (distributed denial-of-service) attacks already. None of the banks with mature fraud controls is willing to wave that particular red cape in front of the foreign criminals.

How can we affect this transfer of risk and responsibility from potential victims to the actual IT operators? In my opinion, regulation should be a last resort. When I studied this crime for the first time, my first thought was to require disclosure--just require that the

---

[15] "The Five Layers of Fraud Prevention and Using Them to Beat Malware". Gartner. http://my.gartner.com/portal/server.pt?open=512&objID=249&mode=2&PageID=864059&resId=1646115&ref=Browse

risk of online banking be disclosed to the small- and medium-sized enterprise customer, and have them agree in writing to take the losses if their PC is hacked. However, it is hard for me to see this requirement doing anything but generating a flight to safety by the depositors and/or a flight from offering online banking by small- and medium-sized banks. I would greatly prefer that the processors and willing banks step forward and simply shoulder the responsibility and then compete with each other on price and end-customer convenience.

Another non-legislative step in the right direction is to find a way to remind all government officials at the local, state, and federal levels, who make decisions on where taxpayer monies will be deposited, that they have a duty not to allow said funds to be stolen. This means no taxpayer funds could be directly or indirectly (e.g., an advance payment to a private contractor) being deposited at any F.I. where "shared responsibility" is their policy.

I believe we could get almost all existing victims made whole if public fiduciaries took the position that if any customer of a given bank has ever lost a dime to account takeover, even if they have signed a settlement agreement over the matter, no taxpayer money may be put at risk there, regardless of what new policy/security measures had been put in place since. In theory, it's possible that the losses from account takeover might be too large for a small bank to bear, but if this has ever truly happened, it has just been once. If necessary, restitution could be limited to some fraction of the bank's reserves.

The Federal Reserve has in the past imposed policies I don't agree with on America's financial services institutions by making it known that it would not approve a merger or acquisition where a bank not complying was on either side of the transaction was not in compliance. If there were any acceptable Fed power, getting banks to drop "shared responsibility" and adopt the stronger security measures their processors have been trying to sell them for years would be one.

But really, I have said my piece. The part of the ABA's position that I cannot support is its insistence that it is the prerogative of its member banks' executives to decide which victims get reimbursed what percentage of their losses, or at most it is a matter for the courts. In a contract dispute, the winner typically cannot recover legal costs from the loser, so for most victims a lawsuit would cost more than they would recover. The victims of account takeover cannot see how the decision about what to do about a new and fast-growing crime that picks off randomly unlucky American churches, school districts, public libraries, medical practices, charities, and small businesses can be made by anyone but the elected representatives of the people.

On the other hand, I am confident in my statement that, at the end of the day, the only way to stop account takeover rather than just continue to talk about it (and also litigate about it), is to concentrate the actual operation of online banking systems in the hands of a smaller number of organizations that answer to the description of the processors I give above. The very largest banks, most especially the ones that provide adequate security, are their own online banking processors. But even if the Congress enables the FFIEC to

issue its Guidance to the 13 processors as well as banks that run their own online banking, at least we will be subtracting more regulation than we are adding. The 14 pages of the FFIEC 2005 Guidance, plus the 8 pages of the 2011 Guidance plus Gartner's 10 pages about the five layers of fraud controls and the security products that fit within them would have to be read and understood by only 13 big companies rather than their 5,000+ small- and medium-sized bank customers.

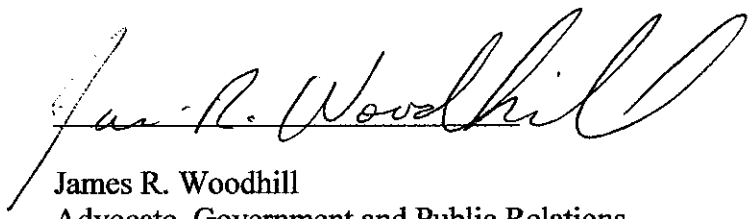
The bad news is that if you do nothing, I can assure you the problem will only get much worse and very soon.

The good news is that among all the complex, difficult, deeply partisan and often controversial problems that lay at your feet everyday; this one—this problem, though very serious and very dangerous is also:

1. Very non-partisan and
2. Very fixable by bright and dedicated people like yourselves.

My only request is that you fix it now, before more money flows to our enemies and becomes too big to fix.

Thank you very much for, first, holding this important hearing. And secondly, thank you for allowing me to participate.



James R. Woodhill
Advocate, Government and Public Relations
YourMoneyIsNotSafeInTheBank.org

Relevant recent testimonies:

FBI Assistant Director Gordon Snow Testimony –

http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

In his September 14, 2011 testimony before the Subcommittee on Financial Institutions and Consumer Credit, Assistant FBI Director Gordon M. Snow presented the authoritative account of ACH fraud, among many others.

Entrust CEO/President Bill Conner Testimony –

http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=9250

The testimony of Bill Conner, President and CEO of Entrust, before the Subcommittee on Communications and Technology of the House Committee on Energy, entitled "Cybersecurity: Threats to Communications Networks and Private---Sector Responses", on February 8, 2012, offers details of this crime and how it is intertwined with the general problem of reliably establishing the identities of actors in cyberspace.