Legal Report and Lead Article originally included only in email version.

The Legal Report

Richard L. Field, Esq.
field@pipeline.com

Mr. Field is an attorney and legal consultant in Cliffside Park, New Jersey, U.S.A. He is a member of the ABA Science and Technology and Business Law Sections. He participated in the drafting of the ABA Digital Signature Guidelines discussed in this report, and co-chairs its Electronic Commerce Payment Committee.

It is fitting that I am writing this first report on legal and Internet banking and commerce issues on Christmas day. For some, this day is about new beginnings. The Journal of Internet Banking and Commerce, and the information era, are also standing at the cusp of something fundamentally new, but not yet quite defined.

Others have long seen this season for its commercial possibilities. Financial reports on our collective shopping purchases this month will be used to diagnose the economic health of entire countries, and serve as the basis for legislative and fiscal policy agendas throughout the upcoming year.

So I thought I would start with another mainstay of the season, the year-end recap. In particular, this report will review some of the past year's activities within the American Bar Association (ABA) to study and promote electronic commerce. It will be a good starting-off point for future legal discussion.

For those of you who are unfamiliar with it, the ABA is a private, voluntary membership association of U.S. attorneys. Others can join as associate members. Despite its unincorporated status, it takes a leadership position on many of the legal issues of the day. Its reports and views have long been used by legislators, attorney practitioners and others.

The ABA is huge and bureaucratic. Most of its membership comes from attorneys in the fifty state bar associations. But, separately, it is also composed of numerous special interest committees, sections and divisions. Among these sub-groups,

the Section of Science and Technology and the Business Law Section have taken notable leadership positions in developing the law of electronic commerce.

The Business Law Section has been studying the current U.S. commercial law, much of which is embodied in the Uniform Commercial Code (UCC) and the laws of evidence, and recommending changes necessary to enable electronic commerce. Some of these efforts include:

(i) a rewrite of Article 2, the law of sales, to cover software licensing;
(ii) the possible elimination of the 300-year-old Statute of Frauds, which requires certain contracts to be "in writing"; and
(iii) a model bank-customer agreement for commercial electronic funds transfers, which follows the basic structure of the 1991 U.S. statute in this area, Article 4A.

The Section of Science and Technology has been looking at the technical side of electronic commerce law. Its Information Security Committee has recently released draft Digital Signature Guidelines. A three-year collaboration of leading legal, cryptography, business and government experts, the 101-page Guidelines are available for download from the Electronic Commerce and Information Technology Division's webpage at "http://www.intermarket.com/ecl". Bound paper copies are available for US$15 from the Section of Science and Technology of the American Bar Association, 750 North Lake Shore Drive, Chicago, Illinois 60611, U.S.A. Telephone: (312) 988-5599; electronic mail: sciencetech@attmail.com. The Information Security Committee worked closely with the State of Utah, which in May 1995 enacted the world's first Digital Signature statute.

The Division has also worked to develop a new U.S. legal specialty, which it calls the "cybernotary". Based on European/Canadian/Mexican notary models, the cybernotary would assume the risks of party identity in an international electronic commerce transaction, while certifying the validity and enforceability of the transaction. There has been substantial collaboration in this endeavor with the International Union of Latin Notaries (UINL). The U.S. Council for International Business (USCIB), which is the U.S. arm of the ICC, has recently created a Cybernotary Association to carry out these efforts. Both the Guidelines and the Cybernotary are based on X.500 and X.509 standards for Public Key Infrastructure and certification authority certificate and key management.

Finally, the Electronic Commerce Payment (formerly Financial EDI) Committee has been discussing, through its committee listserv, fundamental legal issues in electronic commerce payment: from the creation of money, to privacy/anonymity, money laundering, export of encryption, and escheatment of

abandoned property. It has published a model financial EDI trading partner agreement (also available through the ABA), and is working on an equivalent model agreement for the use of debit transfers in EDI.

The ABA will continue to work at the forefront of these evolving issues. Stay tuned for details. And have a good year, everyone.

The Citibank Affair: A Purely Russian Crime?

Nahum Goldmann
ARRAY Development
Nahum.Goldmann (at) ARRAYdev.com>
http://www.ARRAYdev.com/

Nahum Goldmann has been employed as a manager, scientist and lecturer in leading industrial high-tech firms and academia. Mr. Goldmann has published several critically acclaimed books that deal with knowledge transfer issues.

Novoye Russkoe Slovo (NRS), a NY-published newspaper which acclaims itself as the largest Russian-language daily outside of the x-USSR, published an engaging account of the so-called Citibank Affair in September 1995. A fairly large article ("Purely Russian Crime..." NRS, Sept. 15, 1995, pp. 13-14) was written by Vladimir Strizhevsky but was actually based on the original investigative materials submitted by several contributors from Moscow and St. Petersburg, as well as from NY, London, Brussels and other world financial capitals.

Undoubtedly, NRS have done quite a good job in clarifying and illuminating the background of the Citibank Affair. For whatever reasons, the English-language media have not covered the background of Russian participants that well. However, an expert in electronic banking and commerce on Internet might find utterly fascinating the very minute details of this complex crime scheme that involved many people and spread across several continents.

The story at NRS starts at the end of August, 1994 in Tel-Aviv. A certain Alexei Lachmanov, a Georgian national and a holder of a false Greek passport to the name of Alexios Palmidis, had been arrested by Israeli police when he tried to withdraw nearly US$1M. The funds in question were electronically transferred to five Israeli banks from Invest-capital, an Argentinean subsidiary of the Citibank. The Israelis had been tipped by the Citibank through the FBI with the information that all the money transfers had been done with the illegal use of Invest-capital's own secret codes.

The subsequent multinational investigation has shown that it was a leading St. Petersburg's, Russia computer expert Vladimir Levin who

was able to conduct numerous electronic transfers from several Citibank's subsidiaries in Argentina and Indonesia to various financial institutions in San Francisco, Tel-Aviv, Amsterdam, Germany and Finland. According to NRS's speculations, Mr. Levin's succeeded so well because, in addition to Citibank's own electronic cash-management hub in NY, he was also able to crack down the electronic defense of several SWIFT's branch offices in the third-world countries. SWIFT, a secretive Belgium-based electronic telecommunication consortia of World-leading banks, is primarily involved in mutual settlement payments amongst its members.

On the other hand, in the interview with an NRS correspondent V. Kaminsky, Citibank's spokesman rejected the newspaper's version of SWIFT's penetration. Instead he claimed that Citibank knew all along about Mr. Levin's infiltration, playing with him a sophisticated multistep deception game. Of course, the Citibank's face-saving version of events sounds not that convincing, taking into account a large number of uncontrollable players, a sizable amount of real cash involved, multicontinental reach of the overall crime scheme and the fact that the bank was ultimately unable to recover a substantial chunk of its own money.

Not your ordinary self-taught hacker, Mr. Levin, 31, an aloof man and a graduate of a prestigious Department of Applied Mathematics, was considered somewhat of a computer genius in the St. Petersburg's University circles. The scheme started when Mr. Levin's acquaintance, a Russian-American wholesale trader, asked him to develop programming support for his international trading business.

According to Mr. Levin's university friends, the idea of breaking into secure bank networks has been born somewhat spontaneously during a purely technical discussion on the advantages and disadvantages of different bank networking programs. The debaters were members of a St. Petersburg's group of elite computer experts that could best be described as a local response to the Internet's own Cypherpunk community. I found it fascinating and somewhat ironic that the infiltration plot had actually started as a low-key bet that the Russian famous resourcefulness would triumph where the famed Yankee ingenuity has already proven to be unsuccessful!

In the overall crime scheme, Levin was supported by as many as 30 collaborators, at least some of them computer experts. Several of his partners-in-crime, arrested in the U.S., Russia, Israel and the Netherlands, were primarily involved in cash retrieval and laundering, ultimately the most vulnerable part in any grand scheme of electronic theft. It is hardly a secret that most professional bankers are routinely trained to contest, or at least report to authorities, any suspicious withdrawal of large sums of cash. Some of the U.S. arrests have been successfully kept in secret for many months, for the fear of alerting the criminals back in Russia. Mr. Levin himself was arrested in September 1995 in a UK airport, en-route through that country.

Apparently, in the best tradition of this fledging industry, Citibank

have already used the lessons obtained from Mr. Levin's penetration to beef up the security of its own electronic payment system.