

Authors:**William Resnik**

bill.resnik@klgates.com

+1.206.370.7628

Holly K. Towle

holly.towle@klgates.com

+1 206.370.8334

Henry L. Judy

henry.judy@klgates.com

+1.202.778.9032

Sean P. Mahoney

sean.mahoney@klgates.com

+1.617.261.3202

K&L Gates includes lawyers practicing out of 35 offices located in North America, Europe, Asia and the Middle East, and represents numerous GLOBAL 500, FORTUNE 100, and FTSE 100 corporations, in addition to growth and middle market companies, entrepreneurs, capital market participants and public sector entities. For more information, visit www.klgates.com.

Wave of Online Banking Fraud Targeting Businesses

Over approximately the past year businesses have been experiencing an increased level of cyber-attacks designed to steal and misuse the user names and passwords to online banking accounts. Online thieves have been tapping into business bank accounts and ordering fraudulent wire transfers and Automated Clearinghouse (ACH) transactions, often to accounts in foreign countries from which recovery is very difficult. While this type of crime is not new, there are two novel aspects: the increasing sophistication of the hacking software and the nature of the counter-measures that are being recommended. Washington Post writer Brian Krebs provides a chilling and up-to-date view and a recent Forbes magazine article outlines how this development is impacting businesses. See links below to these articles and for more background information.

Which Businesses Are Most Vulnerable?

These attacks are having a special impact on small and medium sized businesses that have banking relationships allowing online transfers of funds via wire transfer or ACH transactions. According to the referenced articles, the thieves often identify the company's controller or other person responsible for initiating wire transfers or ACH transactions. They then send that person a seemingly innocuous e-mail message containing a computer virus that, once opened, installs malicious code (malware) on the computer used to initiate online banking transactions. This is commonly known as a "spear-phishing" attack. Alternatively, the malware simply enables the thieves to locate the networked computer that is used for that purpose, in which case it is not even necessary to know initially the identity of the person responsible for initiating wire transfers or ACH transactions. The malware allows the thieves to learn user names and passwords necessary for use of the online banking applications that access the bank accounts of the business. With this information the thieves are able to steal funds from the business's bank accounts, frequently cleaning out balances in a matter of hours or days, and sometimes triggering advances on over-draft lines of credit. Hackers have been able to move hundreds of thousands of dollars out of the accounts of individual businesses, despite best efforts to maintain security. Increasingly, the malware is able to compromise even security tokens and authentication techniques that are more sophisticated than user name and password. Also the protection provided by strong passwords is no longer available when the virus installs a keystroke logger.

Why Are Businesses Legally Vulnerable to these Attacks?

The online banking transactions of consumers are protected by a Federal statute, the Electronic Funds Transfer Act (EFTA). The EFTA and its implementing regulation (Regulation E of the Federal Reserve Board) limit the consumer's exposure to fraudulent transfers to a maximum of \$50 as long as the consumer promptly reports suspected fraudulent activity. These statutory and regulatory protections are consumer protections and do not apply to accounts of businesses.

Article 4A of the Uniform Commercial Code (UCC) governs allocation of fraud losses arising from funds transfers for business accounts. Under the UCC, fraud losses will normally fall on the business customer if its bank has adopted commercially reasonable security procedures, the business and bank have agreed to use such security procedures to verify the authenticity of payment orders initiated in the name of the business, the bank has in fact employed those security procedures, and the bank has acted in good faith and in compliance with any written instructions of the customer restricting acceptance of payment orders initiated in the customer's name.

What Can a Business Do to Protect Itself from Online Banking Fraud?

One way for a business to reduce its exposure to online banking fraud is by seeking to obtain its bank's agreement to use especially rigorous security procedures to avoid fraud losses. This is easier said than done, however. Sometimes especially rigorous procedures are not available because of higher investment costs in security infrastructure or other reasons. Sometimes they are available, but may not be practical for doing business. In addition to these trade-off issues, both the bank and the customer face the uncertainty that experts disagree on the extent to which enhanced procedures will actually work to prevent or minimize the hacking risk. So what's a business to do? A number of procedures may be helpful to consider:

1. Businesses should consider requiring "out of band" protections, i.e., protections that do not depend solely upon computers. An example would be a transmission that is unlikely to be spoofed (e.g., fax confirmation of the order from a particular fax number or bearing a signature matching the signature card or call-back verification). Banks and businesses will need to discuss what "out of band" procedures are available, practical and affordable, all in light of the corresponding risks to each party.
2. Businesses might consider a requirement that more than one authorized person in the business participate to initiate large fund transfers.
3. Under UCC Article 4A, a business could contract with its bank in writing, or issue written

instructions pursuant to such a contract, to allow only funds transfers below some reasonable limit to be initiated in the customer's name online. Many of the fraud losses to date have been the result of very large transfers of funds by online thieves, greatly out of line with the day-to-day funds transfer needs of the businesses. Frequently a business may have initiated genuine wire or ACH transactions of only less than five or ten thousand dollars per day, but the thieves may submit payment orders for several hundred thousand dollars. Had the business contracted to limit wire or ACH transactions to its accounts to some specified amount in line with its day-to-day banking needs, the majority of fraudulent wires could have been avoided. In this regard, note that under UCC Article 4A, "written" does not include email or other electronic communications and literally means paper. This result has not been changed by the Uniform Electronic Transactions Act (UETA) or the federal Electronic Signatures in Global and National Commerce Act (E-SIGN) because those enabling statutes for electronic commerce exclude Article 4A. Whether a court will so construe Article 4A in all situations, such as when an agreement is offered only online or when instructions are only accepted online, remains to be seen.

4. Because hackers have used e-mail messages containing viruses, or have been able to infect a business' computer while the user was surfing the internet, businesses should consider using a dedicated computer for online banking applications, i.e., one that is not used for surfing the internet or accessing e-mail messages. The American Bankers Association has recently suggested a similar solution.
5. It is important that businesses promptly, frequently, and carefully monitor their online banking activity. Some banks' fund transfer agreements require that fraudulent activity be reported in as little as 24 hours, and failure to report in the time specified in the bank's agreements may cause the business to bear the fraud losses entirely. Banks are also sometimes able to reverse fraudulent funds transfers if they are very promptly reported.

Apart from these specific suggestions, businesses need to be generally proactive in setting up their online banking relationships so that they are structured in a way that optimizes their approach to dealing with the risks of online banking fraud. This optimization requires a balancing act on the part of the bank and the bank's customer because UCC Article 4A's rule regarding reasonable security procedures is a double-edged sword: On the one hand, it does not shield the bank from liability for unauthorized transfers unless the bank offers commercially reasonable security procedures. On the other hand, if the offered security procedure is reasonable, the business will be bound by it, which gives rise to the need to be proactive.

Hence, a central question is what are reasonable security procedures? Litigation has started on that question. In *Shames-Yeakel v. Citizens Financial Bank*, 2009 WL 2949500 (ND Ill. 2009, slip copy), the court would not dismiss on summary judgment a claim that the bank's use of single factor authentication constituted unreasonable security. The plaintiff business claimed that the bank had negligently failed to move from single to dual factor authentication per regulatory guidance in time to prevent the unauthorized transfer at issue. The case did not resolve that issue and focused on other claims such as a claim that the bank was negligent by violating a regulation or by failing a duty not to disclose information concerning one of its customers. However, the court observed: "If this duty not to disclose customer information is to have any weight in the age of online banking, then banks must certainly employ sufficient security measures to protect their customers online accounts." The issue of what constitutes commercially reasonable security procedures as between a bank and a

business customer is currently being litigated in the U.S. District Court for the District of Maine in the case of *Patco Construction Co., Inc. v. People United Bank d/b/a Ocean Bank*.

The reality is that penetrating security systems, no matter how sophisticated, has become a full-time occupation for some very skillful online thieves. Another reality is that businesses and banks benefit from the convenience and efficiencies of online banking. Therefore, unless unachievable perfection is to get in the way of the good, all parties are left with trying to establish and contract for reasonable security and appropriately to allocate losses created by third party criminals. Reasonableness rather than strict liability seems to be the right approach. The challenge here is to evolve the specifics of that reasonability so that banks, businesses and the payment system as a whole are adequately protected.

Please contact any of the authors listed for help with addressing these issues or if you find that your business has been the target of the type of fraud described above. Very prompt action once online banking fraud has been discovered can greatly reduce losses.

The following online articles may be of interest on this topic:

http://voices.washingtonpost.com/securityfix/2009/10/fbi_cyber_gangs_stole_40mi.html?hpid=sec-tech

<http://www.forbes.com/forbes/2009/1116/investing-internet-security-hacker-is-your-online-bank-account-safe.html?partner=email>

Anchorage Austin Beijing Berlin Boston Charlotte Chicago Dallas Dubai Fort Worth Frankfurt Harrisburg Hong Kong London Los Angeles Miami Moscow Newark New York Orange County Palo Alto Paris Pittsburgh Portland Raleigh Research Triangle Park San Diego San Francisco Seattle Shanghai Singapore Spokane/Coeur d'Alene Taipei Tokyo Washington, D.C.

K&L Gates includes lawyers practicing out of 35 offices located in North America, Europe, Asia and the Middle East, and represents numerous GLOBAL 500, FORTUNE 100, and FTSE 100 corporations, in addition to growth and middle market companies, entrepreneurs, capital market participants and public sector entities. For more information, visit www.klgates.com.

K&L Gates is comprised of multiple affiliated entities: a limited liability partnership with the full name K&L Gates LLP qualified in Delaware and maintaining offices throughout the United States, in Berlin and Frankfurt, Germany, in Beijing (K&L Gates LLP Beijing Representative Office), in Dubai, U.A.E., in Shanghai (K&L Gates LLP Shanghai Representative Office), in Tokyo, and in Singapore; a limited liability partnership (also named K&L Gates LLP) incorporated in England and maintaining offices in London and Paris; a Taiwan general partnership (K&L Gates) maintaining an office in Taipei; a Hong Kong general partnership (K&L Gates, Solicitors) maintaining an office in Hong Kong; and a Delaware limited liability company (K&L Gates Holdings, LLC) maintaining an office in Moscow. K&L Gates maintains appropriate registrations in the jurisdictions in which its offices are located. A list of the partners or members in each entity is available for inspection at any K&L Gates office.

This publication is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.