

WIRED IN – WIRED OUT; International Crime Rings Target U.S. Law Firms

By Mark Albright and Troy Fox

The email memo arrives at the law office, and sounds like many others that arrive during the day soliciting legal services. A potential commercial client, albeit located overseas, needs some legal assistance collecting on debts from their customers located in the U.S. They may be willing to pay on a contingency fee basis or hourly basis. They explain that generally their slow paying customers will pay once counsel is obtained in the U.S. and a little bit of pressure is applied. It makes sense, the law firm sends off a client fee agreement and it comes back signed. Later names and addresses, and perhaps telephone numbers of several customers located in the U.S. arrive at the law office. Due diligence performed by the law firm on the internet indicates that the new client is a major manufacturer in Europe or Asia. The web pages of the customers are similarly impressive. A telephone call indicates that the slow paying customer is willing to pay the client via the law firm. The cashier's check arrives shortly. It seems to be a potentially lucrative client for the lawyer.

Then the scam kicks into high gear. The client, located overseas, desperately needs the funds for some major deadline approaching, perhaps to pay suppliers to meet new orders. With the cashier's check from the customer in the bank after several days, the law firm doesn't hesitate to wire the funds over seas, often to a bank in China. The law firm, just to be extra cautious, waits three days to make sure the check clears, and perhaps even has its own bank call to verify that the funds exist in the customer's account. Then disaster strikes. It is later discovered, days, weeks or even months after the check is deposited in the law firm's trust account, that the check was a counterfeit, or worse, a forgery, which explains why both banks involved thought it would clear. Depending upon how many days have transpired, the conspirators, in what is likely a large international organized crime ring, have disappeared. The funds were probably wired out the moment they arrived in an Asian or European bank to who knows where, making it difficult, if not impossible to trace the money, let alone trying to freeze the account by court order. The law firm desperately tries to locate counsel in the city where the funds were wired to, but it is difficult to locate an attorney willing to act immediately due to time zone and language differences. The cost of Hong Kong counsel often exceeds the rates charged by large New York firms. The depositor bank in Asia refuses to voluntarily place a hold on the account without a court order due to the local banking laws and customs. Indeed, due to privacy concerns, most Asian banks will not even voluntarily acknowledge if the funds even exist without a court order.

The law firm has been the victim of a growing scam targeting litigation and collection attorneys throughout the U.S. It's a new twist on an old scheme, which has most of the appearances of a legitimate collection case. The crime ring must create and maintain sophisticated web pages for both the fake client and the fake customers. It must have people available to answer phone calls placed from the law office to either the client or the defendant/customer. But with call forwarding, this is a simple matter and the phones may be answered anywhere in the world, perhaps in an empty room in Shanghai or Hong Kong. With Court delays of just two or three days, the money has usually disappeared, along with the participants in a well oiled crime ring, who are ready to send hundreds of new emails soliciting hundreds of new unsuspecting lawyers throughout the Country. The danger of the scam is that it can change and mutate into hundreds of apparently legitimate variations and locations; a movie producer in Japan hasn't been paid by customers in New York, a furniture manufacturer in Taiwan needs to recover unpaid invoices from a retailer in Chicago, a jeweler in London needs a letter sent to Los Angeles, a pipe supplier in Germany needs just a phone call to his customer in Denver.

Organized check fraud has been on the rise. A report from the American Bankers Association in 1994 found that from 1991 to 1993, dollar losses to financial institutions because of fraudulent

checks and other negotiable instruments rose to \$815 million annually. Major financial institutions attribute at least half of that total amount to organized groups. At least one source has found that more than 1.2 million worthless checks are accepted for payment every day. Many of the organized groups, while also involved in white-collar crime, drug crimes, and even violent crimes, find check-fraud crimes to be what are considered "safe" crimes because it carries a low risk of being caught and minimal penalties even if they are caught.

There are some red flags that law firms should be aware of so they can avoid being a victim of this organized crime. One of the red flags to watch for is that neither the client nor its customer resides in the same jurisdiction as the attorney. That would make it too easy for the law firm to send a runner over to the local address to verify the authenticity of the addresses and business locations.

Another flag to watch out for is a swarming effect. It seems that often, once a law firm expresses an interest in or signs up one of the scammers, additional scammers almost immediately begin contacting the firm. An FBI agent in Cleveland Ohio reported that law firms in Ohio have lost between \$100,000.00 and \$500,000.00 apiece from these types of scams. (Sheryl Harris, The Plain Dealer, "Law firms defrauded in collection scam" Dec. 5, 2007). The end result of this swarming behavior is that a single law firm could easily receive several large counterfeit or forged checks within a single week. The plan of the conspirators is to have all of the funds wired overseas before the unsuspecting collection attorneys discover the fraud. Given the large amount of money involved with each of these checks, even the largest of law firms can be devastated by these scams.

So why don't either US or foreign banks catch this problem more often? The biggest reason is that the checks not only look real, but they seem to be from accounts that actually have the funds necessary to support the check. Both the receiving and paying bank have no reason to suspect the checks aren't going to clear. It isn't until the customer of the account contacts the bank claiming they didn't approve of the check, that any bank is aware of the forgery. So how much time does a person have to bring the forgery to the attention of the bank? The answer is covered by the Uniform Commercial Code (UCC). The UCC 4-406 does impose on the customer a duty to "exercise reasonable promptness in examining the statement [from the bank] ...to determine whether any payment was not authorized because of an alteration of an item or because a purported signature by or on behalf of the customer was not authorized." U.C.C. 4-406(c). So what is reasonable promptness? Well further down in section 4-406(f), the code says:

"Without regard to care or lack of care of either the customer or the bank, a customer who does not within one year after the statement...[is] made available to the customer discover and report the customer's unauthorized signature on or any alteration on the item is precluded from asserting against the bank the unauthorized signature or alteration." (emphasis added)

While "reasonableness" in the code is almost always situational, at least one interpretation that some banks hold is that the customer has up to one year to discover the forgery. Now this might seem an unfairly large time, and in many circumstances it is. However, one must remember that in very large companies, even \$500,000 errors might not be discovered until annual accounting or audits. The UCC keeps the bank at risk for up to one year because the customer may report the unauthorized signature for up to one year after the customer receives the statement. The bank passes that risk onto the customer law firm.

Sadly, there isn't much a law firm can do to protect themselves from these scams, or recover if they have been a victim of one of these scams. While there is insurance for third party fraud, it may be cost prohibitive for many firms.

If the firm has been a victim of one of these scams, it may be possible to hire counsel overseas. However, that too may be cost prohibitive for many firms.

It is usually appropriate to contact the Postal Inspector's Office, specifically the Fraud Complaint Unit, because most of the times the fraudulent cashier's checks have come through the mail. Also, contacting and filing a complaint with FinCEN (the Financial Crimes Enforcement Network) may lead to investigation into these types of crimes. However, these crime rings are extremely difficult to defeat because they are multi-headed. Even when one member is sued, or when one member of the ring goes on the run and is identified by federal authorities, the rings continue to operate. They will continually move their bases of operation, which makes it difficult for authorities to pin them down. One firm recently sued the owner of the key account in Hong Kong, which caused the local member of the ring to flee the jurisdiction. Nevertheless, other members of the ring, at other locations and in other jurisdictions, continued to solicit U.S. law firms, using the same bogus clients and customer names.

The crime rings spend so much time and effort into creating the web pages, client lists, contact information, etc., that they do whatever they can to keep going. Once a group knows they have been detected and are being investigated or if they discover that the name they are using has been identified as a fraud, they simply make changes to the names they are using. Instead of redoing an entire web site, they simply change the name and the domain and continue using the same page layout they have already developed. They will also change the name of the alleged company that is soliciting the law firm, and re-register names, company information, and e-mail addresses.

However, such changes do provide another potential red flag. When a soliciting company has an e-mail address that is a generic free e-mail ending like yahoo.com or hotmail.com, this should raise a red flag. Most companies now have their own domains that are more easily traceable than free yahoo, hotmail or other free e-mail services. Another red flag to watch for is that the scammers often mail the law firm a cashier's check from Canada, making it more difficult for the authorities to trace.

An additional possible solution would be to send a check as opposed to wire money. This will buy the firm some time to conduct more of an investigation. It also gives the bank more time to confirm the cashier's check. If a fraud is discovered, then the firm can put a stop payment on the check, hopefully before the money has disappeared. Prudence would dictate that a firm list in its agreement that no check will be issued on deposited funds for 45 days. This does not provide a 100% guarantee of detecting fraud, but generally provides enough time for the banks to ascertain whether the negotiable instrument is a possible forgery or counterfeit.

Perhaps the best solution for a law firm to adopt is a "wired in – wired out" policy. That is, a law firm policy that only money that has been wired in will be wired out to customers, particularly to new clients located overseas. While this may make some transactions more difficult, it also provides some protection from being victimized by this type of collection fraud. Nevertheless, one type of new scam for money laundering targets law firms, where the overseas clients request the firm to collect monies from subsidiaries and wire to Asia. Hence, law firms need to be constantly vigilant to protect against not only scams but money laundering schemes as well. Such a policy should be written into the retainer agreements which any law firm uses with new clients, especially overseas clients. Exceptions can be made for long term clients the law firm knows and trusts. If a new client is unwilling to accept such a term, then it might be better to simply not do business with that particular client.

Reprinted by permission of Mark Albright and Troy Fox