Beware of Fraudulent Electronic Funds Transfers

By: Deanna Salo and Roger Reitz

There has been an increase in electronic funds transfer (EFT) fraud being committed on small to medium-size businesses in the last year. If your company processes wire transfers through its bank accounts, it is important to be aware of the risks of fraud from both outside and inside the company.

Thefts from outside the company have been perpetrated by cyber thieves who gain access to a company computer and then authorize EFT wire transfers out of the company's bank account. A typical cyber theft is perpetrated by hijacking a company's computer by accessing it through a malicious software program which gains access through an email attachment or an unintended web browsing download. Once this malicious software gains access to a company's computer, it can gain access to the computer's EFT authorization features with the company's bank and then the cyber thief will authorize funds to be transferred to an account controlled by him, typically to a bank account outside the country. Since the authorization is coming from the company's computer, the bank's system may recognize it as a legitimate authorization to transfer funds.

There are a variety of control features which can be used to reduce the risk of such fraud. Some are listed below.

Some banks give the bank customer a pager device, which is used by the company's individual in charge of authorizing wire transfers. The pager device displays a temporary PIN number, which changes every minute of the day. This PIN number would be required to authorize an EFT transfer.

It is important for the company's computer system to be protected by a firewall as well as antivirus and malware protection. This includes the desktops/laptops used in the office as well as the server systems supporting the network. Firewalls should be initiated at both levels of your overall computer system.

Use of a dedicated bank clearing account is another control feature. The clearing account would be established to do all EFT transactions. A 'just-in-time system' could be set up whereby the company transfers the exact amount of funds for the EFT out of its operating account into the dedicated clearing account and then immediately makes the EFT transfer to the outside transferee from the clearing account. This allows the funds to be in the EFT dedicated account only for a short time thereby reducing the timeframe in which the funds are susceptible to cyber theft. All other company bank accounts in this control scenario should not have the capability of transferring funds outside the company.

An EFT authorization system could be set up with the bank whereby one company individual initiates the transaction and another individual is required to authorize it. Another authorization control would be to set up authorized vendors (transferees) with the bank so that the bank will complete an EFT only if it is to a pre-authorized vendor (transferee) that had been set up prior to the requested transfer. Management would determine which company individual(s) would be authorized to set up approved vendors with the bank, to initiate an EFT transaction, and to approve the transaction.

continued on next page

Another control feature at the company level would be to dedicate a computer only for online banking, which is not also used for email, web-browsing, or other such on-line activities. As an additional control a "run as needed" bootable CD that cannot be contaminated by a virus or malware could be used for the "dedicated" computer.

Additionally, management could check the company's insurance coverage to determine if it is covered for such EFT fraud and understand the coverage limitations.

A bank confirmation sent to a designated company employee immediately upon the bank's completion of an EFT transfer can serve as a fraud prevention feature.

Whatever management's decisions are with regard to controls over EFT's, it is important to keep in mind that the time frame to inform a bank of a fraudulent EFT transfer is very short. EFT's (electronic funds transactions) do not fall under the same legal protection as ACH transactions (automated clearing house). A fraudulent EFT transfer can be completed by a cyber thief and the money transferred into a foreign bank account in less than an hour. If not reported within this time frame the company might not have legal protection to recover the money if the bank itself is not able to recover it. In any case, it is advisable for someone within the company to reconcile EFT transactions from the bank to the company's records on a daily basis.

Many of the control features mentioned above can reduce the risk of fraud perpetrated by company personnel as well as fraud perpetrated by cyber thieves from outside the company. Company management, with consultation from their bank, is in the best position to determine which control features are available and which are optimal for the company to implement. Such decisions would be based on company management's assessed risk of both external and internal EFT fraud and such factors as the cost of the control features, the nature of the company's EFT transactions, the company's computer system, and the company's personnel who would be authorized to use the system.

SOURCE: Journal of Accountancy Oct 2010

If you would like assistance in evaluating your company's exposure to EFT fraud or in determining other control features which can be implemented for your company's EFT activity, please contact Deanna Salo or Roger Reitz. We are here to assist the FBC in any way we can.

continued on next page

CRAY, KAISER LTD.

CERTIFIED PUBLIC ACCOUNTANTS
AND CONSULTANTS TO BUSINESS

Deanna Salo, CPA
Cray, Kaiser Ltd.
1901 S. Meyers Road
Suite 230
Oakbrook Terrace, IL 60181
Phone: (630) 953-4900 x210
Fax: (630) 953-4905
Email: dsalo@craykaiser.com

Roger Reitz CPA, CVA
Cray, Kaiser Ltd.
1901 S. Meyers Road
Suite 230
Oakbrook Terrace, IL 60181
Phone: (630) 953-4900 x213
Fax: (630) 953-4905
Email: rreitz@craykaiser.com

We are a full-service accounting and business advisory service with three offices in the Chicagoland area. With over 25 professionals on staff serving clients across the Midwest, we have the size to meet your needs and the personal service to exceed your expectations.

Locations

Oak Brook
1901 S. Meyers Road
Suite 230
Oakbrook Terrace, IL 60181
Phone: (630) 953-4900
Fax: (630) 953-4905

Joliet
1000 Essington Road
Joliet, IL 60435
Phone: (815) 725-2946
Fax: (815) 744-1681

Chicago
Monadnock Building
53 West Jackson Street
Suite 828
Chicago, IL 60604
Phone: (312) 880-0927
Fax: (312) 880-0944