Secure Your Bank Accounts!

a special report by John C. Stucky

TrinSoft llc

trinsoft.com

Secure Your Bank Accounts!

by John C. Stucky

Over the last year or two I have been involved in a higher number of fraud or bank account "scares" than normal. One of these events caused me to dig deeper into the rules and regulations regarding corporate bank account security, and I was very surprised at what I found:

1. **ACH and Wire Transfer fraud rules are very different than credit card rules.**
2. **The burden is on the account holder.**
3. **The allowable time to detect and report is much quicker than I thought.**

We have all dealt with credit card chargebacks, fraud and misuse. The issues I am describing are NOT credit card related. You will need to work with your bank and processor to understand your credit card rules and the best security practices around those transactions.

I am referring to ACH (Automated Clearing House) or Wire Transfer transactions. These transactions are automatically initiated and touch your account directly. Today, virtually anyone can initiate an ACH deduction from your bank account. All they need is your account number and the ABA or Routing Number (which is easily found for any bank – it is public information). Any individual who has seen one of your printed checks has all the information they need to initiate an ACH withdrawal.

The surprising news is that most banks require you – the account holder – to detect and notify them within 24-48 hours of a possible fraudulent transaction or you are completely liable! Yes, you read that correctly – you have 24 hours to detect a fraudulent electronic ACH transaction or you are liable for the loss. Different banks have different rules, but doing some research on my own of several local and larger banks in this area, I found this timing to be very consistent.

The surprising news is that most banks require you – the account holder – to detect and notify them within 24-48 hours of a possible fraudulent transaction or you are completely liable!

This was alarming to me when I discovered it last year. As a result, I started to research some best practices to help secure corporate bank accounts. There are many sources of information on this topic. The Conference of State Bank Supervisors is one great source of information and they even published a paper on this topic which you should be able to read here:

*https://www.csbs.org/ec/cato/documents/**bestpractices**cato.docx*

For those of you who are short on time and want a quicker to-do or checklist, here are a few things I discovered and some next steps for you to consider:

1. Contact your bank(s) and get a clear explanation of their policies and fraud reporting period requirements for each type of fraud (credit card, ACH, Wire Transfer, …). You should also ask them if they will provide suggestions or advice on their services and best practices.
2. Restrict and/or consolidate your disbursement accounts to as few as possible.
3. Implement the Positive Pay service from your bank (almost all banks offer this service).
4. Reconcile and review your bank accounts daily if possible (no later than weekly). The time of monthly bank reconciliations is in the past. You need to reconcile more frequently.
5. Secure all on-line logins and passwords and restrict user access to only those functions necessary.
6. Follow standard internal controls regarding the segregation of duties and be sure more than one person in your organization is helping to handle and reconcile the accounts.
7. Review your insurance policy and talk to your agent about what coverage you currently have for bank fraud and what is available.

Reconcile and review your bank accounts daily if possible (no later than weekly). The time of monthly bank reconciliations is in the past. You need to reconcile more frequently.

I have been the victim of bank and credit card fraud, and I suspect most of you have, too. It is no fun to go through it, and with the ease with which automated systems can initiate on-line and electronic transactions, it is more important than ever to implement good security and controls. If you have questions about any of these items or would like to implement some of these practices with our software, please drop us a line and we will help in any way we can.

John C. Stucky

jstucky@trinsoft.com

859.252.6225 x. 1013

linkedin.com/in/johnstucky

About TrinSoft

As a trusted partner, we help companies automate processes and transactions to be more efficient and save money. We work with Microsoft Dynamics, document management solutions and unique, custom applications. Our goal is always the same – help companies be more profitable by improving their information management.

trinsoft.com | trindocs.com | trinsoft-it.com

With the ease with which automated systems can initiate on-line and electronic transactions, it is more important than ever to implement good security and controls.