Business Law Update November 2013

PUBLISHED ON

November 2, 2013

TABLE OF CONTENTS

Protecting Your Bank Account From Fraud - A Cautionary Tale
Dodd-Frank Update: How to Qualify for the End-User Exception to the Mandatory Clearing Requirement
De Facto Merger Doctrine and Successor Liability under Pennsylvania Law
Addressing Digital Assets in Estate Planning

Protecting Your Bank Account From Fraud - A Cautionary Tale

By: Kimberly J. Decker

Most people have heard of "Phishing" and are aware of other scams used by hackers to fraudulently gain access to bank accounts, credit cards and other assets. While common sense and security measures can help prevent scammers from getting this information, most people don't realize that the power to debit an account is contained in every check for that account!

When you make an online payment by authorizing a third party to debit your account electronically (whether by entering your account number and your bank's ABA routing number online, or providing it over the phone), you are essentially "writing" an electronic check. Making electronic payments this way is quick, easy and convenient. But what happens when someone else uses your account number and bank ABA routing number to pull money from your account?

Business accounts are more at risk than personal accounts because personal accounts benefit from federal limits on the losses they can be made to bear. Business accounts, however, enjoy no such protection. There are two typical fraud scenarios faced by a business - fraudulent transactions made by its own authorized employees, and fraudulent transactions made by unauthorized persons, whether employees or not. Generally speaking, a bank is not required to refund a business for its loss from a fraudulent electronic debit if the transaction was made by a person who was authorized to access the account (presumably an employee). In that situation, the business really only has a claim against the employee - but in many cases, the money is long gone. As a result, the business often ends up bearing the loss unless it has insurance that will cover the loss.

If the unauthorized debit is initiated by a person who is not an authorized signer on the business account, the business may be able to get the money back through a reversal of the transaction it if moves quickly enough - typically within 48 hours, which requires incredible watchdog efforts. If the transaction can't be reversed, the business may be able to recover the money lost from the bank if it can show that the bank failed to follow agreed procedures to authenticate transactions. However, if the bank's security procedures were commercially reasonable and the bank completed the transaction in good faith, the bank is still not responsible to repay the business.

As you can see, recovery from the bank in this situation is often difficult (if not impossible). So what can a business do to protect itself?

• Identify the extent of your risk in this area - what is the likelihood that you could be subject to a scam of this (or any other) nature, and what protection do you have in place to prevent this from happening?

• Don't allow one person to have sole access to sensitive information and accounts.

• Promptly notify the bank when authorized signers are fired or leave their employment.

• When terminating the employment of individuals who have had access to sensitiveinformation, you are better off barring them from the premises after they are fired.

• Review bank statements and transactions and reconcile them frequently so that unauthorized transactions are caught quickly.

• Review existing bank relationships. Know your rights and responsibilities for fraudulent transactions under existing bank account agreements.

• Ask your bank about available fraud detection plans. Most banks offer various types and levels of fraud detection support that can prevent this type of fraud (as well as other scams) from being successful.

• Determine whether current insurance policies would provide coverage for fraud of this type and if not, whether such coverage is worth buying.

Back To Top

Dodd-Frank Update: How to Qualify for the End-User Exception to the Mandatory Clearing Requirement

By: Daniel T. Desmond

On September 9, 2013, many interest rate swaps and credit default swaps entered into by non-financial commercial end-users became subject to the mandatory clearing requirement imposed by Title VII of the Dodd-Frank Act. However, if you are a non-financial company that utilizes swaps to hedge and mitigate commercial risk, there is an exception to the mandatory clearing requirement called the "end-user exception." Virtually every entity that qualifies has elected the exception since the process of clearing swaps can be complicated and very expensive. Electing the exception can therefore save a lot of time and resources. This article outlines 1) the criteria necessary to determine whether you qualify as an "end-user," and 2) the steps necessary to elect the end-user exception.

I. Is Your Company an End-User?

In order to qualify as an end-user, your company must meet the following conditions.

1. It is not a "financial entity" as defined in Section 2(h)(7)(C)(i) of the Commodity Exchange Act. The term "financial entity" includes swap dealers, major swap participants, commodity pools, employee benefit plans, and banks that have total assets greater than $10 billion. Banks that have total assets under that amount qualify for the end-user exception, even if their larger parent bank holding company may not. Captive finance companies meeting certain thresholds may qualify, as well.

2. It uses a swap to hedge or mitigate commercial risk, as defined under CFTC Regulation 50.50(c). In order to constitute "hedging," the swap must be a) used to reduce the overall risk of market fluctuation, b) consistent with the company's overall hedging and risk mitigation strategies, and c) entered into by the company at the time a position is first executed.

3. It generally meets its financial obligations associated with entering into uncleared swaps.

4. It takes certain governance steps if it is a public company (see Part II).

5. It reports the information described in steps 1-4 to a swap data repository (SDR), or to the CFTC if no SDR is available, through an annual filing that would cover swap transactions taking place over the upcoming year. While most companies are expected to make the annual filing, CFTC rules offer the option of reporting the required information on a swap-by-swap basis. See Part II for more information about this filing.

II. How Does Your Company Elect the Exception?

1. If you are a public, SEC reporting company, there are certain corporate governance requirements that you must first follow.

(a) The board, or an "appropriate committee" of the board, must review and approve the company's use of uncleared swaps. The approval, which may be in the form of a resolution, must authorize the company to enter into swaps that will not be cleared and will not be executed on a facility or exchange. A committee is "appropriate" only if it is specifically authorized to review and approve the decision to enter into swaps. Therefore, if the committee does not currently have that authority, then it must be authorized either by amending the committee charter or adopting resolutions to give the committee the authority.

(b) Board or committee approval can be affected on an annual basis because public companies must include confirmation of the approval each year as part of the annual filing. Approval also can be obtained on a swap-by-swap basis and reported to an SDR in connection with each swap transaction.

(c) The review/approval requirement applies to the reporting issuer and to any entities controlled by the issuer, including non-reporting subsidiaries. The reporting company's board has reasonable discretion to determine the appropriate committee for approving decisions on swaps for its subsidiaries or affiliates.

(d) The board or committee must "set appropriate policies" governing the use of swaps subject to the end-user exception and review the policies annually, or more often if there is a significant change in management's policy towards its swap trading strategy. Companies can comply with this requirement by having the board or committee review and discuss with management its swap policies.

(e) The board should update board or committee calendars and agendas to include an annual review of company policies on the use of swaps and approval to enter into uncleared swaps if applicable. Additionally, the board or responsible committee should stay in contact with management regarding any significant changes that occur in its trading strategy which might alter its hedging strategy.

2. Complete and file the "Annual End-User Clearing Exception Form" with the Depository Trust & Clearing Corporation (DTCC). This form requires you to make several representations that are necessary to confirm your status as an end-user. First, you must confirm that your company is not a "financial entity." Second, you must state that your company enters into swaps in order to hedge or mitigate commercial risk. Third, you must state how your

company meets its financial obligations associated with entering into uncleared swaps. Options include written credit support agreements, pledged assets, guarantees from other parties, as well as your own company's available financial resources. Finally, if you are a public reporting company, you must represent that an appropriate committee of your board of directors, or the board itself, has reviewed and approved the decision to enter into uncleared swaps. An authorized signatory of your company must then sign and certify the accuracy of the foregoing information.

III. What To Do Next

If you have not already done so, it is not too late to elect the end-user exception for future swaps. Barley Snyder has completed this process for several clients, including publicly traded companies and small banks that qualify, and has drafted sample resolutions that your board may tailor to its specific needs. If you plan on executing a swap in the future and have not already taken the steps necessary to elect the end-user exception, please feel free to contact us.

Back To Top

De Facto Merger Doctrine and Successor Liability under Pennsylvania Law

By: Troy B. Rider

Successor liability is an exception to the general rule that, when one entity sells assets to another entity, the assets are transferred free and clear of all but valid liens and security interests. When successor liability is imposed, a plaintiff with a claim against the seller may assert that claim against and collect payment from the buyer. In Pennsylvania, the general rule does not apply and liability attaches to the successor when one of the following is shown: (1) the purchaser expressly or impliedly agrees to assume such obligation; (2) the transaction amounts to a consolidation or merger ("de facto merger"); (3) the purchasing corporation is merely a continuation of the selling corporation; (4) the transaction is fraudulently entered into to escape liability; (5) the transfer was not made for adequate consideration and provisions were not made for the creditors of the transferor; or (6) the successor undertakes to conduct the same manufacturing operation of the transferor's product lines in essentially an unchanged manner. The successor is then strictly liable for injuries caused by defects in the product line, even if previously manufactured and distributed by the transferor (commonly referred to as the "Product Line exception").

Four factors are analyzed in determining whether the de facto merger exception applies: (1) continuity of ownership, (2) cessation of ordinary business by, and dissolution of, the predecessor as soon as practicable, (3) assumption by the successor of liabilities ordinarily necessary for uninterrupted continuation of the business, and (4) continuity of the management, personnel, physical location and general business operations.

In the traditional asset purchase transaction between unrelated parties, the second, third and fourth factors are often present. Accordingly, the absence of the first factor (continuity of ownership) is all that prevents a de facto merger and the purchaser being liable for the obligations of the seller. Until 2009, Pennsylvania law required courts to consider all four factors, but a de facto merger finding did not require that all four factors were present. The Pennsylvania Superior Court, in a 2009 case, established the primacy of the continuity of ownership factor by holding that if the owners or the seller do not have an ownership interest in the purchaser, the transaction is not a de facto merger and, accordingly, the purchaser is not liable for the seller's obligations. In 2012, the Pennsylvania Supreme Court vacated and remanded the Superior Court's 2009 decision in *Fizzano Brothers Concrete Products, Inc. v. XLN, Inc., et al.*, 42 A.3d 952 (2012).

In *Fizzano*, the Supreme Court held that continuity of ownership is still required for a de facto merger, but broadened the confines of what constitutes continuity of ownership to include a "stockholder interest." Unfortunately, the court did not define "stockholder interest." *Fizzano* specifically dealt with a construction company trying to collect on a $114,000 judgment obtained against a company that sold its assets to another unrelated company. The Supreme Court did not opine on whether a de facto merger occurred but rejected the Superior Court's analysis of the continuity of ownership element, and focused on a comparison to statutory mergers under Pennsylvania law. Because in a statutory merger the sellers can receive consideration other than stock, the Supreme Court held that the same is true for the de facto merger exception. In other words, continuity of ownership may be satisfied if the owners of the selling business have some type of interest in the purchaser (i.e. a "stockholder interest") even though the owners of the seller and the purchaser are not identical.

Due to *Fizzano*, sellers and purchasers should be cautious in structuring transactions to avoid any potential successor liability. Ideally, future decisions will help delineate what constitutes a "stockholder interest" but until then, the saga of successor liability continues.

Back To Top

Addressing Digital Assets in Estate Planning

By: Brian R. Ott

Working with their advisors, people develop estate plans in an effort to detail how their property will pass to their heirs. With our ever increasing reliance on digital technology and the internet, however, this effort has taken a new twist as an additional type of property emerges. A comprehensive estate plan will increasingly require consideration and management of digital assets.

Questions have arisen in recent years regarding digital assets, ranging from the mundane (what is the password to the decedent's online account?) to the emotionally-charged (who should have access to the decedent's family photographs stored online?). Unfortunately, as is often the case with technological advances, the law has failed to keep up with the issues created by the advancement. Only seven states currently have legislation governing the disposition of digital assets; Pennsylvania is not among them. A legislative proposal regarding the treatment of digital assets was introduced in the Pennsylvania House of Representatives during the 2012 session, but was referred to committee and never acted upon. In the absence of specific legislation, the "Terms of Service" agreements between Internet Companies and the individual creating an account are controlling. These terms vary widely from company to company, but most companies, concerned about privacy issues, describe the user's account as a non-transferable license, personal to the user, which terminates upon the user's death.

Until new laws address the many issues presented by digital assets, individuals should take a number of common sense steps as part of their estate plan. First, a list of digital assets, along with passwords and other information necessary to access the accounts, should be created. This list should be readily accessible, but maintained in a document separate from the person's will, since the will likely becomes a public document upon death. Some procedure or safeguard should be implemented so that the existence and location of the list is known and only designated persons have access to it. The will itself should include provisions regarding the disposition of digital assets, even though it is currently unclear whether such provisions will be legally binding. Individuals should consider saving photographs and other data they want passed to heirs to a hard drive or other storage device that can be backed up, to the extent that there is no license infringement in doing so. Finally, if the Internet Company allows multiple account holders, consideration should be given to setting up an account which is jointly owned by your heirs to avoid access issues.

In all likelihood, the next several years will see the passage of legislation which will provide clarity to those seeking to pass ownership of their digital assets to their heirs.

Back To Top