

IN THIS ISSUE

- > Landlord Waivers & SNDAs— Everybody's Favorite Documentation Task
- > Regulatory Agencies Renew Commitment to Internet Security

The Bank & Finance Group at Fredrikson & Byron represents a wide spectrum of clients in the financial services and commercial areas including banks, bank holding companies, insurance companies, and clients with banking affiliations. Our attorneys have substantial knowledge in state and federal banking regulation, enforcement actions, tax law, bank mergers and acquisitions, litigation, bankruptcy, commercial paper, secured financing, real estate, and UCC matters.

For more information and contacts within the Bank & Finance Group, see page 4. An electronic version of this newsletter is available on the Internet. You can access our home page at www.fredlaw.com. FredNEWS: Bank & Finance is edited by Jane C. Ball, Senior Paralegal.

main 612.492.7000
fax 612.492.7077

www.fredlaw.com

Offices / Minneapolis
/ Bismarck
/ Des Moines
/ Fargo
/ Monterrey, Mexico
/ Shanghai, China

Member of the
World Services Group
A Worldwide Network of
Professional Service Providers

Landlord Waivers & SNDAs – Everybody's Favorite Documentation Task



Sjur Midness
612.492.7311
smidness@fredlaw.com

When the economy is thriving, it is a rare occurrence for a borrower to default on its loans so profoundly that its secured lender needs to repossess its assets. It is even rarer for a commercial landlord to suffer such a profound loss of cash flow that it cannot service its mortgage debt and ultimately loses the property to its mortgagee. Consequently, few in the industry were well practiced in either scenario in 2008. After the past couple of years, however, we are all too familiar with these situations, though, in some cases, we wish we had better documentation to make the repossession process proceed more smoothly.

LANDLORD WAIVERS

If a borrower/tenant defaults and its lender, as a secured party, opts to repossess inventory or equipment, it is important for the lender to have a clear agreement in place with the borrower's landlord that explains the following:

1. The landlord does not have any claim on the borrower's assets (or any claim it does have is subordinate to the lender).
2. The lender has the right to enter the property as necessary to repossess the borrower's assets.
3. The lender is responsible only for rent extending through the reasonable time during which it is executing its repossession rights or arranging for a sale, plus any damage it causes during that time.

Without these provisions, it is likely the lender will end up fighting about these issues with the landlord, which slows down the repossession process and makes it more expensive. Contracting for the above provisions up front sounds simple enough, so why is it that lenders do not always do so? Answer: Landlords do not like to agree to these provisions because they are a pure giveaway of rights without receiving any value.

Further, obtaining these agreements from the landlord can be costly for the borrower/

>LANDLORD WAIVERS & SNDAS – EVERYBODY'S FAVORITE DOCUMENTATION TASK CONTINUED

tenant. Landlords with strong leverage can charge legal fees to the borrower/tenant for the cost of having the landlord's counsel review the proposed agreement. These landlords may also charge a processing fee or extract some other costly concession in exchange for the landlord's consent.

And because landlords dislike these agreements, negotiations can take a lot of time. In cases where these agreements are heavily negotiated, they often result in an awkward three-way conversation among lender counsel, tenant counsel and landlord counsel—each trying to avoid responsibility for moving it along. Whoever has the most leverage (usually the lender) generally imposes its will. The borrower/tenant almost always ends up getting caught in the middle.

SUBORDINATION, NON-DISTURBANCE AND ATTORNMENT AGREEMENTS

One major concern for a tenant (and, potentially, lenders who have secured interests in the tenant's property) is that if the tenant's landlord defaults on its mortgage loan to its mortgagee, the tenant could lose its lease rights and be evicted (if the lease is on tenant-attractive terms) or see its rent expense greatly increased. An aggressive mortgagee also could try to obtain property belonging to the tenant (which also may be security for the tenant's loans with its lender) if there is any ambiguity about whether the property belongs to the tenant or is a fixture belonging to the property owner.

It is important in this case to have an agreement in place among the tenant, its landlord, and the landlord's mortgagee to protect the tenant and, in many cases, the tenant's lender. This agreement is typically referred to as a Subordination, Non-disturbance and Attornment Agreement, or "SNDA." First, the SNDA states that even if the landlord defaults and the mortgagee forecloses, the mortgagee will respect the tenant's lease on its terms (Non-Disturbance).

In return, the mortgagee reasonably asks for the tenant's acknowledgment

that, subject to Non-Disturbance, its lease rights are subordinate to the landlord's mortgage (Subordination). The mortgagee will also ask the tenant to acknowledge that it does not own any of the fixtures to the mortgaged property. To the extent there is ambiguity regarding whether any of the tenant's property is a fixture, the tenant will want to ensure this is clarified in the agreement. Finally, the mortgagee will ask the tenant to acknowledge that it will pay rent to the mortgagee after any foreclosure (Attornment).

Again, obtaining such an agreement makes sense, so why do we not see more of them? Answer: They, too, are painful to negotiate. However, since an SNDA may be sought by either the tenant (seeking Non-Disturbance) or the mortgagee (seeking Subordination and Attornment), there often is more common ground to work from than there is with landlord waivers.

TAKEAWAY

Landlord waivers are helpful tools for loans for which equipment or inventory are material collateral. Subordination, Non-Disturbance and Attornment Agreements (SNDAs) are helpful tools when the tenant/borrower has important lease rights or the landlord/mortgagor has existing leases in place. Consider seeking these agreements, but know that it will be a bit of a struggle. ♦

Sjur Midness is an attorney in the Bank & Finance Group.

Regulatory Agencies Renew Commitment to Internet Security



Beau J. Hurtig
612.492.7267
bhurtig@fredlaw.com

Prudent bankers typically attempt to anticipate matters that are likely to receive the greatest scrutiny from bank regulators during an examination. Anticipating particular areas

of examiner focus permits bankers to evaluate these areas beforehand and, if necessary, implement enhancements. Over the past three years, bank examiners often placed heightened emphasis on matters such as capital levels, asset quality and liquidity; however, recent experiences indicate that new areas of emphasis may be on the horizon.

One such area in which financial institutions should be ready for increased scrutiny is internet security. Based on the Federal Financial Institutions Examination Council's (FFIEC) recent release of its "Supplement to Authentication in an Internet Banking Environment" (Supplementary Guidance) and the rise in internet related financial fraud, we believe that the security of internet banking products may be one emerging point of emphasis in examinations.

BACKGROUND

As you may recall, the FFIEC initially issued enhanced security techniques with respect to internet banking in 2005. On June 28, 2011, the FFIEC renewed its commitment to internet banking security by issuing the Supplementary Guidance. The FFIEC summarized its reasoning for updating the 2005 guidance by stating, "The agencies are concerned that customer authentication methods and controls implemented in conformance with [the initial 2005 guidance] several years ago have become less effective."

The Supplementary Guidance confirms the recommendations to banks offering internet products that were outlined

CONTINUED ON PAGE 3 >

in the original guidance. These recommendations include employing layered controls and multifactor authentication with respect to certain high risk transactions, as well as conducting periodic risk assessments. As a reminder, high risk transactions are “transactions involving access to customer information or the movement of funds to other parties.” Layered security “is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control” such as fraud monitoring systems, dual authentication, out-of-band verification, and positive pay.

In addition to reaffirming the benefits of these previous recommendations, the Supplementary Guidance provides additional commentary regarding the effectiveness of certain security measures and minimum expected internet security program elements based on the FFIEC’s experience with fraudulent activity since the issuance of the initial 2005 guidance.

RISK ASSESSMENT

The Supplementary Guidelines reaffirm the importance of periodic risk assessments, stating that “financial institutions should perform periodic risk assessments and adjust their customers’ authentication controls as appropriate in response to new threats to customers’ online accounts.” These risk assessments should be performed at least every twelve months.

The risk assessment should consider relevant factors, such as those related to (i) the external threat environment, (ii) the customer base utilizing the institution’s internet banking products, (iii) product functionality, and (iv) the institution’s actual experiences with fraudulent or other malicious behavior. Financial institutions also may benefit from maintaining records regarding the risk assessment, its findings, and resulting enhancements the institution implemented so that examiners may readily see the steps the institution has taken to maintain security.

AUTHENTICATION FOR HIGH RISK TRANSACTIONS

The Supplementary Guidelines require layered security for high risk transactions initiated by both consumer and business customers. Importantly, the FFIEC also makes an important distinction between internet transactions initiated by consumers and those initiated by businesses. Specifically, the FFIEC acknowledges that consumer transactions generally pose a relatively lower risk of fraudulent activity due to the lower frequency and smaller size of the transactions. Conversely, the FFIEC recognizes that due to the frequent initiation of larger ACH and wire transfers, business transactions (primarily those initiated by small to medium size institutions) pose a greater risk. Therefore, in addition to layered security, the Supplementary Guidelines recommend multifactor authentication with respect to business transactions.

Significantly, the Supplementary Guidelines indicate that the agencies expect layered security measures to contain certain minimum elements. Such strong language setting forth minimum requirements is rare in interagency guidance, so financial institutions would be wise to implement these requirements.

The first element the agencies expect is a process designed to detect and respond to irregularities relating to initial login and transaction initiation. The agencies also share their experience that manual or automated transaction monitoring or anomaly detection and response “could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer’s established patterns of behavior.”

The second element the agencies expect involves enhanced controls for system administrators on business accounts. Such enhanced controls on the program administrator might include an additional authentication routine or transaction verification routine prior to final access

or program changes (e.g., calling or faxing your customer to notify them of the proposed change in access or the program).

QUESTIONABLE AUTHENTICATION TECHNIQUES

The Supplementary Guidelines are also helpful in that they specifically describe certain security processes that the agencies may not view as sufficient. The first is the use of simple device authentication, which involves the loading of a single cookie on a customer’s computer to confirm the computer is related to the party’s initial enrollment, username, and password. The Supplementary Guidelines state that the agencies no longer consider simple device authentication to be sufficient. However, the use of more complex device authentication techniques, including those that consider a combination of factors—such as computer configuration, IP address, geo-location, and other factors—are still sufficient.

The agencies similarly do not consider the use of simple challenge questions in the event that the primary login technique becomes unavailable to be sufficient (e.g., mother’s maiden name, high school, graduation year, etc.). Instead, financial institutions are directed to employ more sophisticated “out of wallet” questions that involve answers not readily available on the internet or other public domain. Further, the Supplementary Guidelines recommend asking multiple questions and including a “red herring” question that the customer will recognize as nonsensical but that may trick a fraudster.

CUSTOMER EDUCATION PROGRAM

Finally, the agencies recognize that customer education may play an important role in mitigating internet related fraud. Therefore, the Supplementary Guidelines recommend educating both consumers and businesses regarding internet security, including the internet banking protections the institution offers (and does not offer),

CONTINUED ON PAGE 4 >

BANK & FINANCE GROUP

ATTORNEYS

Eric S. Anderson.....	612.492.7030
Katie L. Cole.....	612.492.7288
Clinton E. Cutler.....	612.492.7070
Emily E. Duke.....	612.492.7097
Lynn M. Gardin.....	612.492.7102
Thomas W. Garton.....	612.492.7021
Karen L. Grandstrand.....	612.492.7153
Mark W. Greiner.....	612.492.7140
Beau J. Hurtig.....	612.492.7267
Leah C. Janus.....	612.492.7349
Jenna K. Jenson.....	612.492.7384
Paul B. Jones.....	612.492.7111
Douglas W. Kassebaum.....	612.492.7292
Mary M. Krakow.....	612.492.7164
Keith A. Libbey.....	612.492.7010
Debra J. Linder.....	612.492.7163
Kimberly A. Lowe.....	612.492.7324
John W. Lundquist.....	612.492.7181
David R. Marshall.....	612.492.7154
Sjur Midness.....	612.492.7311
Sherrill R. Oman.....	612.492.7131
Mary S. Ranum.....	612.492.7072
Robert K. Ranum.....	612.492.7067
Karla L. Reyerson.....	612.492.7418
John A. Satorius.....	612.492.7023
Thomas F. Steichen.....	612.492.7338
Jon E. Strinden.....	701.237.8202
Robert B. Whitlock.....	612.492.7011

SENIOR PARALEGALS

Jane C. Ball.....	612.492.7033
Bonnie A. O'Malley.....	612.492.7093

FredNEWS: Bank & Finance is prepared by attorneys at the law firm of Fredrikson & Byron, P.A. to report on legal developments in the fields of banking and finance. It is not intended as legal advice. Readers should not act upon the information contained in this publication without professional counsel. Please feel free to call one of the attorneys or paralegals listed above if you have any questions. No portion of this publication may be reproduced or used without express permission. For further information, please contact Melissa Kjolsing via e-mail at mkjolsing@fredlaw.com. For address changes you may also e-mail Melissa or fax updated information to her at 612.492.7077.

To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code, or (ii) promoting, marketing, or recommending to another party any matters addressed herein.

© 2011 Fredrikson & Byron, P.A.

Fredrikson
& BYRON, P.A.

200 South Sixth Street
Suite 4000
Minneapolis, Minnesota
55402-1425

>REGULATORY AGENCIES RENEW COMMITMENT TO INTERNET SECURITY CONTINUED

the situations under which the institution may contact the customer with respect to login credentials, if any, suggestions for customer risk assessments, a listing of risk control mechanisms customers may want to employ, and/or bank contacts to whom customers should report suspicious activity.

TAKEAWAY

Bankers may wish to consider reexamining their internet authentication security procedures, as this area is likely to become a point of particular emphasis for examiners in upcoming exams. ♦

Beau Hurtig is an attorney in the Bank & Finance Group.

announcement



Sjur Midness rejoins Fredrikson & Byron as an officer practicing in the firm's Bank & Finance, Mergers & Acquisitions and Private Equity Groups. Sjur works with clients in financing transactions, loan restructurings, and mergers and acquisitions. Sjur's background includes debt and equity capital markets transactions and credit facilities for whole loan portfolios and commercial real estate. Sjur can be reached at 612.492.7311 or smidness@fredlaw.com.



Jenna Jenson is an associate in Fredrikson & Byron's Corporate, Bank & Finance, and Mergers & Acquisitions Groups. Jenna focuses on negotiating and documenting commercial financings and mergers and acquisitions, dispositions, and restructuring transactions, as well as commercial loan, lease financing, and structured finance transactions. Jenna can be reached at 612.492.7384 or jjenson@fredlaw.com.

