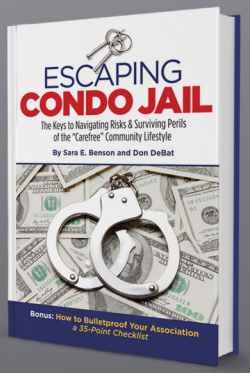
How to Bulletproof Your Association's Biggest Asset:

THE MONEY



Life-saving Excerpts from ***Escaping Condo Jail*** by Sara Benson and Don DeBat.

Welcome to our standard operating procedures handbook for condominium and homeowner associations.

The pages that follow are excerpted from the appendix of our book *Escaping Condo Jail*. In it, we outline the keys to navigating risks and surviving perils of the "carefree" community lifestyle.

While this handbook focuses on financial duties and responsibilities, we hope it proves useful to all owners as well as board members with specific financial roles in association management.

Moreover, with the contents of this handbook, we hope to begin a trend to greater transparency in association operations. We also hope to open communications to benefit the four out of five real estate transactions that association properties now represent.

While we encourage you to buy our book, *Escaping Condo Jail*, please know that in our desire to promote change, many pieces of the book are available for download online at www.escapingcondojail.com

Kind regards,
Sara and Don

The 35-Point Financial Procedures Manual

If you are elected treasurer of your community association and accept the challenge, there are many policies and procedures you will need to learn before you start planning budgets, collecting assessments, and signing checks. Board members and officers of all community associations in America should read the following 35-point list of financial procedures and consider it a survival manual. It is divided into four segments:

- Inheriting Old Books
- Guarding and Vigilance
- Cyberbanking Procedures
- Efficiency Maximization and Return

The Takeover: Inheriting Old Books

1. Incoming treasurers or accounting managers should never accept the recording of financial books or accounts of a previous money manager. In order to be sure there is a clear line between the actions of the prior money manager and the current, a new bank account should be opened and the funds transferred to the new account. The new account helps to draw the line of accountability. Liability is also reduced by the new account, since any old checks that may be lying around will then be invalid.

2. Immediately notify the bank when officers change. Bank signature cards must always be brought current immediately following the annual election. All officers should go to the bank together to provide identification and verify signatures.

3. For incoming treasurers or accounting managers, a "transition document" stating all association account balances—including a statement as to the purpose of the reserve account, all contracts (including the vendors' names and the expiration dates), and any outstanding payments due for services rendered or received—should be provided to the new money manager.

4. Destroy all old checks and deposit slips. Use a cross shredder or a document destruction company.

5. Keep new checks under lock and guard the keys.

6. If a board treasurer or management company refuses to give up the bank accounts (it has happened), send the person or company a certified letter demanding the rightful return of all association property—including the checkbooks. Include a deadline in the letter (i.e., "must be received by [insert date]"). Demand the records be sent within the deadline specified in your state and bylaw governance. If the records are not returned within the time period specified, immediately call the police. Report the checkbooks as stolen property.

Avoiding the Sting: Guarding and Vigilance

1. All board officers should provide copies of their deed and their state identification or driver's license to be kept on permanent file.

2. Always screen employees in advance with a credit and background check. Collusion between association employees and contractors is not uncommon. Be sure to run background checks on all board applicants as well—not just the employees. Associations should amend their governing documents to prevent someone with a prior conviction from serving on the board. Banning felons from handling huge sums of money is a good idea.

3. Always, always, always have at least two sets of unrelated eyes on the monthly bank statements. Regardless of size, informal operations almost always set the stage for fraud. Choose a bank that agrees to issue duplicate monthly statements. For self-managed associations, have bank statements sent not only to the treasurer, but also to another board member who does not have access to the account. If using a management company, one set of monthly bank statements should be sent to the management company and another to a designated member of the board—preferably the treasurer.

4. Require that anyone with access to the association's funds be bonded and have adequate fidelity insurance. Minimum fidelity coverage should be at least three months of assessments plus everything in reserves as the policy limit. Unlike directors' and officers' insurance, fidelity insurance typically covers acts of malfeasance and fraud. Double-check annually that the management company has a fidelity bond for your association.

5. Do not allow the person who issues the checks to be the same individual who reconciles the bank statements.

6. Require board members to review monthly financial statements within 10 days of receiving them from the bank, and require checkbooks to be balanced within 10 days of receiving statements from the bank. Examine the bank statements and look at copies of any suspicious check to make sure it was deposited by the person or firm to whom the check is made payable.

7. Never allow the management company to have access to reserve accounts.

8. Never accept a computer-generated spreadsheet or financial report in lieu of an actual bank statement. Always insist on receiving the actual bank statement directly from the bank.

9. Require that all budgets, without exception, conform to generally accepted accounting principles (GAAP). Budgets should clearly show a beginning and ending balance of the previous year's bank balances, an income and expense statement of the previous year's bank balances, and projections for the upcoming year's income and expenses.

10. Require computerized financial software be used to keep the books. Financial software such as Quicken can generate reports and spreadsheets that conform to GAAP. Although the reports can be altered, it is easier to compare them to the actual check register. Remember that homemade spreadsheets are the easiest to manipulate.

11. A minimum of two signatures should be required on every check—perhaps even three signatures for amounts over a certain dollar amount, say $2,500. Signatories must never sign blank checks, even "in case of an emergency." No exceptions!

12. Never allow association credit or debit cards to be issued or used since they only require one signature.

13. Require invoices and receipts before paying bills. Never allow payments to be made without an invoice and a receipt.

14. Use "safety check" stock with watermarks and "warning bands." Keep in mind that it is now so easy to Photoshop, alter, or duplicate checks to change dollar amounts or the payee's name that even an 8-year-old can do it.

15. Consider using bank products such as Positive Pay—an automated fraud-detection tool offered by most banks that matches the account number, check number, and dollar amount of each check presented for payment against a list of checks previously authorized and issued by the association. All three components of the check must match exactly or the bank will not pay it. When Positive Pay is used together with a highly secure check, Positive Pay can dramatically cut fraud losses.

16. Hire an accountant to conduct periodic audits—not just a "financial review"—of the association's accounts. Require that the audit be performed at least every five years, or more often as required by state statute, and that an annual statement from a licensed certified public accountant (CPA) be prepared. If anyone is thinking of stealing, he or she will know that a review or audit is being done on a consistent basis. So, he or she will think twice about it.

17. Keep an eye on the amount in the reserve account. Should money in the reserve account exceed FDIC limits, require that an additional account be opened at a different, unaffiliated financial institution.

Banking on the Cloud: Cyberbanking Safeguards

1. Prepare a written procedure on how accounts are safeguarded. This plan should include everything the association is doing to prevent fraud and theft. It may include locking up checks in a safe, buying a dedicated computer, and having dual controls in place. Having the procedure in writing enables associations to prove that they have taken due care under the Uniform Commercial Code, which may provide additional protections under the law.

2. Have a completely dedicated computer for financial transactions. This computer must not be allowed to surf the web, open e-mail, go to Facebook or Twitter, or chat online in any form whatsoever.

3. Run the most up-to-date operating system, and buy good antivirus and antispyware protection and keep it up to date. If banking online, the latest and greatest protection is essential. Scan the computer daily to ensure the system is safe. Also enable firewall protection.

4. When banking on the Internet, web addresses should always contain an '*s*' after the prefix http. Legitimate banking sites will always contain this *s*—as in *https*—which represents secure, or hypertext transfer protocol secure. A secure socket layer transmits an encrypted tunnel system, or channel, between you and the bank. If the website doesn't have an '*s*', it is fraudulent. Every site that deals with money should be encrypted.

5. Initiate a "dual control" payment process with your bank and money manager. Ensure that all payments are initiated from the association's bank accounts only after the authorization of two individuals. One individual authorizes the creation of the payment, and a second is responsible for authorizing the release of the payment. This process should be in place for all banking transactions.

6. Change passwords on a regularly scheduled basis, and never disclose them to outside parties. Put passwords on a calendar—perhaps to correspond with regularly held board meetings. Passwords should be complex—never a word from a dictionary or a name or birth date. Passwords should contain both letters and numbers and, for extra protection, characters such as %, &, *, or @. If necessary, use a password-change chart for the year. The change chart might indicate the rotating password source. Password sources may include—in forward or reverse order—the planets in the solar system, the states in America, the periodic table of elements, the months of the year, types of gemstones, breeds of dogs; however, eliminate one critical letter, such as the second consonant, or the first vowel, etc., to avoid detection by a Trojan dictionary web spider.

7. Always exit the bank's website completely and clear your browser.

8. Consider positive pay exceptions that place an automatic stop on specific types of transactions over certain specified limits—such as $1,000.

9. Check electronic transactions every day. This step is critical because in most cases the bank's ability to reverse wire transfers lasts only a few hours, even when problems are immediately reported.

10. Exercise extreme caution when using mobile devices. Reports of virus and malware in the mobile sector have been steadily increasing. Avoid using any mobile application not endorsed or provided by the bank. Banking applications for mobile phones often come from third-party sources, and the user doesn't know what the application may be doing with the information. If using a mobile phone for any type of banking, configure the application by phone not to save passwords—otherwise, losing the phone or having it stolen could cause a major security breach.

Show Me the Money: Maximizing Efficiency and Return

1. Consider mandatory recurring Automated Clearing House (ACH) payments for assessment payments. This type of payment can track payments in real time—even from an iPhone—and delinquencies can be addressed immediately. To help avoid skimming, do not allow owners to make payments in cash.

2. If the reserve account is substantial in size, the association's financial procedures manual should address how—and whether—the money will be safely invested, for example, in staggered CDs, or a small percentage may be invested in guaranteed investments. All risky investments such as playing the stock market should be strictly prohibited, even if the association's president is a trader.

FINANCIAL PROCEDURES CHECKLIST

Inheriting Old Books

- ☐ Open new accounts.
- ☐ Update bank signature cards.
- ☐ Obtain a transition statement.
- ☐ Destroy all old checks.
- ☐ Keep new checks locked.
- ☐ Report any theft to police.

Guarding and Vigilance

- ☐ Keep board officers' deeds and state-issued IDs on file.
- ☐ Perform credit and background checks on employees.
- ☐ Have monthly bank statements sent to two different people.
- ☐ Require fidelity insurance and bond money handlers.
- ☐ Require that different people write checks and reconcile books.
- ☐ Require board members to review bank statements within 10 days.
- ☐ Never allow the management company to access reserve accounts.
- ☐ Never rely on computer-generated reports instead of bank statements.
- ☐ Require budgets to conform to GAAP.
- ☐ Require use of established financial software.
- ☐ Require two signatures minimum on each check, with amounts over $2,500 requiring three signatures.
- ☐ Never allow credit or debit cards.
- ☐ Require invoices before paying bills.
- ☐ Use safety checks with watermarks and warning bands.
- ☐ For sizable accounts, use an automated fraud detection tool.
- ☐ Perform periodic audits on a schedule.
- ☐ Do not let accounts exceed FDIC limits.

FINANCIAL PROCEDURES CHECKLIST

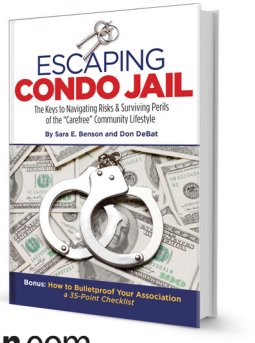
Cyberbanking Procedures

- ☐ Have a procedures manual for Internet banking protocol.
- ☐ Have a dedicated computer for financial transactions.
- ☐ Run up-to-date operating systems and antivirus protection.
- ☐ Ensure financial websites are secure—look for an *s* after http.
- ☐ Require two separate authorizations to process banking transactions.
- ☐ Change passwords on a regularly scheduled basis.
- ☐ Always exit the bank's website completely.
- ☐ Consider Positive Pay with a $1,000 limit.
- ☐ Check electronic transactions every day.
- ☐ Use extreme caution with mobile devices for banking.

Efficiency Maximization and Return

- ☐ Collect assessments using ACH payments.
- ☐ Invest association monies wisely.

Co-authors Sara E. Benson and Don DeBat have made real estate the focus of their professional lives over successful careers that span decades. As a Realtor® and consultant to the U.S. Department of Housing and Urban Development, Sara has built a reputation for being a staunch consumer advocate. Don DeBat's extraordinary experience as a journalist and real estate editor for two major Chicago newspapers adds a passion for uncovering the truth and cut-to-the-chase storytelling to the mix.



Available on amazon.com