



Bexar County IT News

June 2014



Business Improvement: Escheatment

Run Date: 04/01/2014
Run Time: 11:22:28

Bexar County Civil Cash System
Disposd Interest Trust Cases with
No orders/proceedings after: 02/28/2011

Page: 1

PCN: CBE15002
JCL: CBE15004
CTL: CBE15008

POST DATE	CASE NUMBER	PROC. DATE	ORDER DATE	STYLE	BALANCE
05/08/2013	1998CI09245	04/23/1991	04/28/1982	• GERALD D FEY AND MARY FEY INDIV - SUGERMAN BROTHERS	265.49
05/08/2013	1998CI15635	09/25/1984	09/25/1984	• JUAN LEBAL - ALLSTATE INS. CO.	945.59
08/03/1989	1998CI18300	06/18/1993	07/15/1991	• NATL LIFE & ACCIDENT - ROCHELA M DANIELE	1.17
09/29/1997	1998CI11331			ALVILLO	250.00
12/13/2007	1997CI02737			DTY CHANNING DURAN	2,000.00
02/13/1998	1998CI02278			J SHAW, ETAL	100.00
04/01/1998	1998CI04953			RECORDED	200.00
02/04/1999	1999CI01558			- BRANCHIZIO, INC.	500.00
04/09/2003	2000CI04602			TY OF SAN ANTONIO	14,000.00
11/21/2003	2000CI05451			J. KAHLEIC, II	11,260.81
08/01/2006	2002CI08411			IST HEALTHCARE SYSTEM	537.58
01/15/2004	2002CI09642			CARE FUND - TOWERS PE	14,418.53
09/13/2002	2002CI13348			L S CORRIGAN	6,409.00
01/15/2004	2003CI19496				7,844.35
02/06/2004	2004CI01844			THERESA O WOOTEN	500.00
05/28/2004	2004CI08245			- CITY OF SAN ANTONIO	110.00
11/04/2005	2004CI09806			SEOC - ROBERT J KOENIG	500.00
06/08/2005	2005CI09467			E-TEXAS PROPERTY HOLDI	250.00
08/26/2009	2005CI11096			GUTIERREZ ETAL	10,000.00
11/18/2005	2005CI18374			ER SOURCE LTD ET AL	2,500.00
05/22/2006	2006CI02327	09/10/2010	08/31/2007	MARIA C REYNA - HELEN S GONZALEZ	100.00
04/07/2006	2006CI05450	09/10/2010	07/10/2006	PW SERVICES DBA PAGESSETTER PERSONNEL SE - MISSION	500.00
06/09/2006	2006CI08899	08/17/2010	08/17/2010	ALONSO RECALANTE MD DA - KATRINA R CORONA ET AL	100.00
08/03/2006	2006CI10531	05/25/2010	05/25/2010	SPACE POTATO MUSIC LTD ET AL - BOUGAINVILLEA INC E	100.00
09/08/2006	2006CI12744	05/04/2010	02/22/2007	ATAT OPERATIONS INC - STEPHEN J BYE	1,000.00



Escheatment is the process of turning over unclaimed or abandoned property to a state authority. The unclaimed property law requires government entities, financial institutions, and businesses to report personal property they are holding that is considered abandoned or unclaimed to the State. Property is turned over to the Texas Comptroller's office annually when the owner's location is unknown, and the property has been inactive after the suitable abandonment period has expired.

Each year in April, the District Clerk's Office and County Clerk's Office begin the process to escheat funds to the State. In the past, the clerk would have to search the case management system and financial system to determine if a case with funds in the Court Registry was dormant. BCIT created a report to identify the cases with no activity in the last two years. The clerks no longer have to take time finding cases to be escheated—the report does the work for them.

In addition to identifying the cases, BCIT has worked with the teams to develop an escheatment process to update the financial system with the funds escheated to the State. The process mimics the entries that clerks need perform on each case. These entries, which previously took hours, now occur in a matter of seconds.

Mainframe Password - RACF

Keeping sensitive data secure is a high priority for BCIT. We have taken several measures to ensure that the right people have the right access.

Therefore, your ID to the Mainframe (Mocha) will get revoked if you enter the incorrect password four times. Your profile will also get suspended if you have moved to a different position and/or department.

Each department has a security supervisor who can assist with resetting your password if you have been revoked. The Help Desk can also assist with resetting your password 8-5 M-F, 335-0222 and the Computer Room is available 24x7, 335-0100



Handy Android Tips and Tricks



1. **Activate the Android Power Strip Widget.** The single most important feature in Android is its built-in power strip widget. Here, you're able to quickly disconnect all the phone's battery-destroying features, like Wi-Fi, Bluetooth and the Great Batter Killer that is GPS. Long-press on the screen and install it via the widgets category.

2. **Android call screening.** If you're a paranoid call-screener, Android is there for you. Open up the Contacts listing of the person you're currently avoiding, then select Menu > Options. From here you're able to ping all incoming calls from this person directly to voicemail. Give people the brush off with Android.

3. **Organize things into folders.** Fancy a quick Home screen shortcut to your starred favorite contacts? Long-press the Home screen and make it so.

4. **Rename Android folders.** And, once you've done that, to customize things to perfection it's possible to rename folders. Simply open the folder, then long-press on its name in the top bar to bring up the Top Secret renaming field.

5. **Set up your keyboard launch shortcuts.** One of the reasons many people still love their QWERTY keyboards is Google's inclusion of the reliable old keyboard shortcut system in Android. The phone has a completely customizable collection of app launcher shortcuts, which are found under Settings > Applications > Quick Launch.

6. **Set your double-tap zoom level.** On phones that don't support multi-touch zooming, you can take more control of your web browsing zoom via the browser's setting page. Change your view to "Close" if you want the page to fly right into extreme close up when you double-tap the screen, or leave it to "Far" if you're happy to have text only cropping in a little closer when you double-tap.

7. **Add words to the Android dictionary.** This is such a useful feature it ought to be screamed about via a sticker on the phone when you take it out of the box. If you've been laboring through life with a difficult-to-spell name, type it once into your Android phone's text field - then long-press on it in the suggested word field. This adds it to the dictionary, so you'll never have to type more than the first couple of characters of your name again.

8. **Browser combo button.** The Android web browser features a clever multi-function button beside the address bar. While a page is loading it turns into an "X" to cancel loading, but once a page has finished it transforms itself into a bookmark adding and history management tool. It's always there for you.

9. **"What I meant was..."** Not sure what all these smiley faces 🐼 actually mean, press Menu then Insert Smiley while on the Android keyboard - then the meaning of them all is nicely explained.

Top 5 USB Security Risks



USB flash drives are by a landslide the most popular means of making data portable. Well over 150,000,000 USB drives were sold last year according to Gartner. But standard unsecure USB flash drives unfortunately come with a line of built in security risks that every user should be aware of. Here are the top 5 hidden security risks with standard unsecure USB flash drives.

1. Delete Does Not Mean What You Think When it Comes to USB Flash Drives.

When it comes to erasing files the “Delete” button should really read “Hide”. This is what we call the FAT recovery issue. You “delete” a file from your USB flash drive or perform a Quick Format to “delete” all files. What this actually does is comparable to placing a sheet of white paper, as an only safeguard, over the stack of sensitive documents left on your desk. It just erases the reference to the file in the FAT, the [file allocation table](#) that each drive has. The file itself is still there, just in temporary hiding since standard USB flash drives have no reset feature. Using FAT data recovery or repair tools anyone can bring your “deleted” secrets into the daylight again. This could mean embarrassment or catastrophe depending on the data stored.

2. Misplacing a USB Flash Drive For Any Amount of Time is a Real Risk.

When a drive is misplaced, or left out of sight, your data might be tampered with. New USB malware threats spread this way, and even worse is that your stored stuff might have been copied off. You never know, because there is no way telling what has happened when you were off guard. Even if you encrypt your files with a security software the encrypted files could be copied off to perform a what is called a parallel off-line attack with rainbow tables and software tampering software. Even script kiddies can pull things like this off. The files are simply there in the open, available for anyone to fiddle around with given the shortest moment of opportunity.

3. Budget USB Flash Drives Put Your Data at Risk.

If the USB flash drive was too cheap then the flash component part of your USB flash drive is probably fading away at an alarming speed. 8 GB can rapidly fade down to only actually store 7GB and then 6GB, 5GB, 4GB, 3GB. You see the pattern. This will risk the stored files and folders. On the actual flash is where your data is stored. Think of [flash circuits](#) as little boards with millions of little miniature switches on them. Each switch tells the computer a story about the data stored on the USB flash drive. Good flash drives have perfect switches, built to last through a life-time of heavy usage. Low-cost bargain USB flash drives can be equipped with switches that are already broken or will fall off and break after even just one use. This means that the storage capacity of the USB flash drive will die of quickly and that the data stored by the faulty switch can become corrupted. This will mean that the files stored are not secure against data loss. Losing work this way can be costly and very annoying.



(Continued on page 4)

4. Your Unsecure USB Flash Drive Can Set off a Computer Catastrophe.

The Autorun feature that easily can be copied onto any standard USB drive is like a crazy friend that invites thugs with baseball bats to your house warming party. It has no built in judgment whatsoever. Windows Autorun consists of two files. One autorun.inf that is a pointer file directed towards the second, the target executable/program that is to run. And it will run anything, even Conficker which was the malware that highlighted this security flaw. A malicious Autorun configuration can seriously mess up any computer you stick the drive into. The problem is actually so bad that Microsoft removed the Autorun completely for removable storage starting with certain Windows 7 releases.

5. Standard USB Flash Drives Have NO Built in Security Features.

There is no password protection or encryption of the data stored on a standard USB flash drive. This might be OK for the family photos but not for your work related data. If you misplace the unsecure USB flash drive you can cause a breach that sets your company back quite a bit of money. [Globally, over 20,000,000 USB flash drives were lost just last year](#) so you would, sad to say, be in good company. Of course your organization does not want to end up becoming a headline for something as easy to lose as a USB stick.

Did you Know?

- ◇ 60 billion emails are sent daily, 97% of which are spam.
- ◇ 9 out of every 1,000 computers are infected with spam.
- ◇ The first public cell phone call was made on April 3, 1973 by Martin Cooper.
- ◇ Sweden has the highest percentage of internet users (75%).
- ◇ Email was already around before the World Wide Web came.
- ◇ While it took the radio 38 years and the television a short 13 years, it took the World Wide Web only 4 years to reach 50 million users.
- ◇ Amazon originally was a printed book seller company, now it sells more e-books than printed books.
- ◇ 220 million tons of old computers and other technological hardware are trashed in the United States each year.
- ◇ U.S. President Bill Clinton's inauguration in January 1997 was the first to be webcast.
- ◇ Microsoft was originally named Micro-Soft. They dropped the dash in 1976.
- ◇ The first mouse was invented by Douglas Engelbart in 1963. It was a wooden shell with two metal wheels.
- ◇ "Stewardesses" is the longest word that is typed with only the left hand.
- ◇ Yahoo! was originally called 'Jerry's Guide to the World Wide Web'.

