NEWSLETTER

March 2023

Volume 2

Password Resets

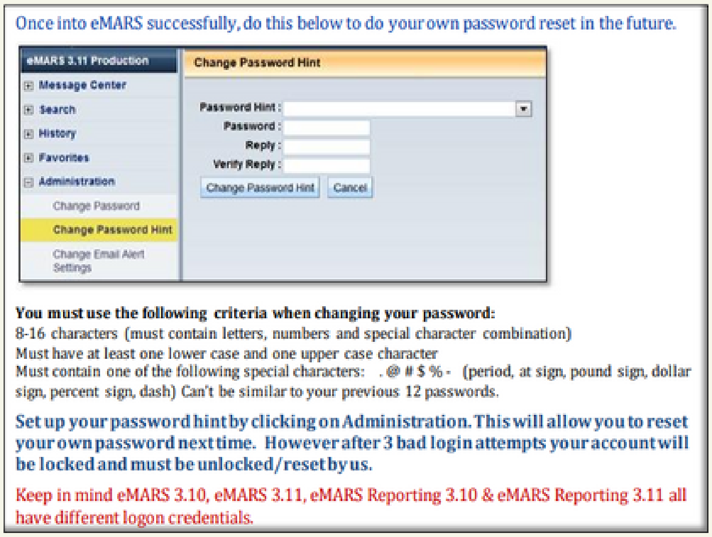
- Send all requests to the Helpdesk's group inbox: Finance.CRCGroup@ky.gov

- In your **Subject line**, please state:
    - Password Reset, **and**
        - 3.11 eMARS, *or*
        - 3.10 eMARS, *or*
        - eMARS Reporting.

- In the email body, **please provide your name and User ID,** if not already provided in your email signature.

Your User ID is **required** for requests to reset eMARS Reporting.

You can save yourself time by setting up a future password reset by following the directions below.



Once into eMARS successfully, do this below to do your own password reset in the future.

You must use the following criteria when changing your password:
8-16 characters (must contain letters, numbers and special character combination)
Must have at least one lower case and one upper case character
Must contain one of the following special characters: . @ # $ % - (period, at sign, pound sign, dollar sign, percent sign, dash) Can't be similar to your previous 12 passwords.

Set up your password hint by clicking on Administration. This will allow you to reset your own password next time. However after 3 bad login attempts your account will be locked and must be unlocked/reset by us.

Keep in mind eMARS 3.10, eMARS 3.11, eMARS Reporting 3.10 & eMARS Reporting 3.11 all have different logon credentials.

Kentucky Vendor Self Service (VSS)

Please encourage your vendors to register themselves on our Vendor Self Service website.

By registering and activating their account on VSS, they will be able to add/update addresses, contacts, and commodity codes for potential business opportunities. If eligible, 1099s will also be available for download soon.

A new look and updated user experience will occur soon, when we launch VSS4. Links to updated user guides will be provided in next quarter’s newsletter and be posted on the VSS Home Page.

Keep in mind - EFT/Direct Deposit updates can only be completed by Finance CRC utilizing the SAS-63 form located here.

** The eMARS financial link connects to Vendor Self Service when outside the COT firewall or on COT VPN.*

Customer Resource Center
Ph: 502-564-9641
Toll free: 877-973-4357
Finance.CRCGroup@ky.gov

Attention:
Property Officers and
Fixed Asset Personnel

The due date for the Annual Physical Inventory of Fixed Assets is **Wednesday, May 31, 2023**.

Only non-expendable personal property is required to be inventoried for State Fiscal Year 2023. You are still required to contact the Auditor of Public Accounts (APA) with your inventory schedule at least 10 days before your inventory begins.

Fiscal Year 2023 Inventory Procedures and Inventory Observation Log Sheet can be found on the Office of the Controller website or by clicking here.

Upon completion of the physical inventory, the following documents are **required** to be returned via e-mail to the Office of the Controller:

- A Certification Letter signed by both the fiscal officer and property officer of your department. This is **required** even if your agency **does not** have any fixed assets $5,000 or greater.
- **One** of the following:
  - A copy of the eMARS Report Fixed Assets – Equipment (ACFR) to meet minimum annual inventory requirements, *or*
  - Fixed Assets – Equipment $500 or over report to inventory all items $500 and above.
- The Inventory Observation Log Sheet listing all documents that are processed during the inventory period for non-expendable personal property,
- Any continuation sheets containing items located during the inventory which exceed the cost thresholds but were not reflected on the report.

You do not have to wait until May to complete your fixed asset inventory. The earlier you begin planning, the easier it will be on all involved! It is highly suggested to begin preparation and planning now and provide procedures and guidance to all who may be involved in the inventory process.

Please read through all instructions before beginning your inventory. If you have questions or need any assistance, please don't hesitate to contact me via e-mail, Microsoft Teams, or by phone. If you are not the correct fixed asset contact for your agency, please let me know as soon as possible so I can send the procedures to the correct person and update my contact listing. I've tried to keep my list as up to date as possible, but I know there are always personnel changes happening.

If you have questions, please contact:

Jessica Pinkston
jessica.pinkston@ky.gov

> If everyone is moving forward together, then success takes care of itself.
>
> HENRY FORD

QUERY FOLDER CLEANUP

Many agencies have a lot of clutter in their query folders. A review of the query folders of various departments reveals many queries that are useless, broken, or duplicative of other queries in the folder. It is in the best interest of the report developers of any one department to work with their agency reporting lead to do some clean-up of report queries. Less clutter will make it easier for report users to select the report query most appropriate, but it will also highlight areas of report need.

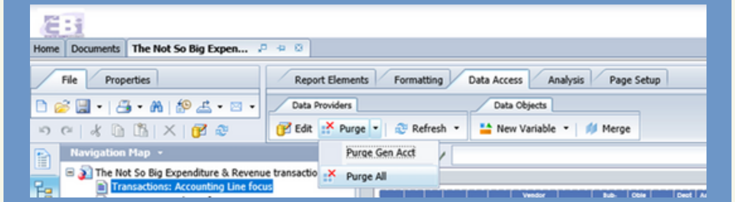
If additional motivation to work on this task is necessary, there's a big eMARS conversion lurking on the horizon, so the more that an agency is able to weed out unnecessary and disabled queries, the less work that will be required in the lead-up to the conversion.

PURGE YOUR DATA

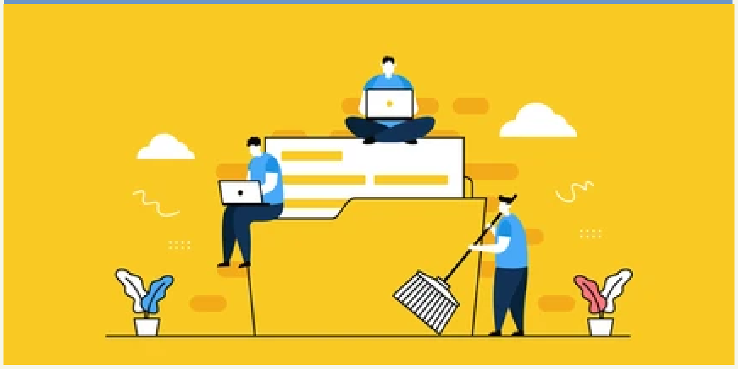
If data is saved on the face of an EBI report query, that information needs to be purged by a report developer. Permanent copies of report results should be exported as PDF or Excel or CSV documents, never saved on the query itself. Allowing data to be saved on the face of the report can cause several problems:

- **Sharing of unauthorized data**
- **Storage cost**
- **System functionality**
- **User confusion**

The Purge Data function is located on the Data Access tab, in the Data Providers sub-tab.

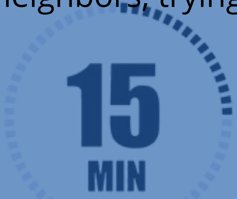


Developers are strongly encouraged to invest a little bit of time every week scanning the department's report inventory for queries that reflect saved data. It is all but guaranteed this will become a hot button topic down the road, so it's a wise course of action to insulate a functional area now rather than later.



HOW TO NOT BE IN THE NEWS

Many people dream of their 15-minutes of fame. But nobody wants a News truck parked outside their house, with reporters stalking them on their errands and harassing their neighbors, trying to find out why they funneled state money to a fraudster/hacker – right?



Of course, right!

But, on any given day, if you work with vendor payments, you run the risk of being that person.

Here’s how: Phishers are using email daily, attempting to persuade you to send them state money. Obviously, they aren’t advertising their efforts. Rather, they are craftily disguising their attempts by hacking vendors and sending you personal emails from vendors you are doing business with every day. They are asking you to change the way you pay them by providing you with new EFT/ACH banking information and asking you to update their payment file with the new information. This will allow all future payments to be received in this manner.

Obviously, if the request was unsolicited by you, it’s more likely to be fraudulent. But what happens when you email the vendor, and they are replying to your email with this new info? That has to be legitimate, right?

A recent event shows how even that interaction, could be fraudulent. In fact, it happened just like that.

A state employee emailed an order to a small vendor in Central Kentucky. The vendor replied to the email the next day with an invoice and new banking information, requesting payments be sent via EFT/ACH to the account information listed in the email.

Thankfully, the state employee had a question and called the vendor. The vendor was confused, stating they had never received the order, definitely didn’t send an invoice, and don’t use EFT/ACH for payments. So, what was going on?

As it turns out, the vendor’s email had been compromised/intercepted and the state employee was emailing directly with a hacker who appeared to be the vendor, as the email was the vendor’s correct email address.

In another similar instance, a hacker gained control of a vendor’s eMARS Vendor Self Service (VSS) login and changed the vendor’s bank account information in eMARS to be directed to the hacker’s account.

So, how can you make sure you don’t end up in the news for sending state money to Fraudsters/Hackers?

Here are three steps:

1. **Never accept banking information from any vendor via email**. If you do, find their master agreement/contract, and reach out to the contact person listed on the contract **via telephone or in-person – never via email**. Confirm the changes. If legit, have them provide the information over the phone or in-person (if possible).
2. **Never confirm a vendor’s banking information by using VCUST in eMARS or by calling the number in the email**. ALWAYS use the master agreement/contract to find contact information to **call and verbally verify** a customer’s banking information.
    a. **Remember**, a hacker who sends you an email will provide their own phone number. Just because you talk to someone who sounds nice doesn’t mean you are not talking to a hacker.
    b. **Remember**, Vendor Self Service (VSS), which feeds the data in VCUST, is data entered by the Vendor (or hacker, in some cases) and is not data from which you should confirm banking information. If you don’t know the vendor personally, you must use the contact info in the master agreement/contract and confirm the information **verbally**.
3. **Never open an attachment (PDF or Word document) or click a link on an email requesting you to change banking information**. Remember, if it’s a hacker, the attachments/links likely contain viruses aimed at crippling the state’s systems. You don’t want to be **that** person who lets them in.
    a. Rather, pick up the phone, dial the **known** number from the contract and speak with someone who can identify their relationship with the state (or someone you know) about the email you just received, to verify its legitimacy.

You may dream of your 15-minutes of fame, but you don’t want to be made famous for being the person who sent millions (or hundreds of millions) of dollars to a hacker/fraudster/phisher. Although COT does a terrific job, you can’t rely on COT or some other government agency to keep the bad guys away.

The bad guys are probably emailing you right now. So, be a little paranoid, stay alert, and reach out if you have questions. Don’t be on the news. 😊

DAILY NEWS
No. 49,725
THE BEST SELLING NEWSPAPER IN THE WORLD
Today's Edition
National - World - Business - Lifestyle - Travel - Technology - Sport - Weather
EXTRA!
EXTRA!
View from the top
The best way to get something done is to begin
Economy

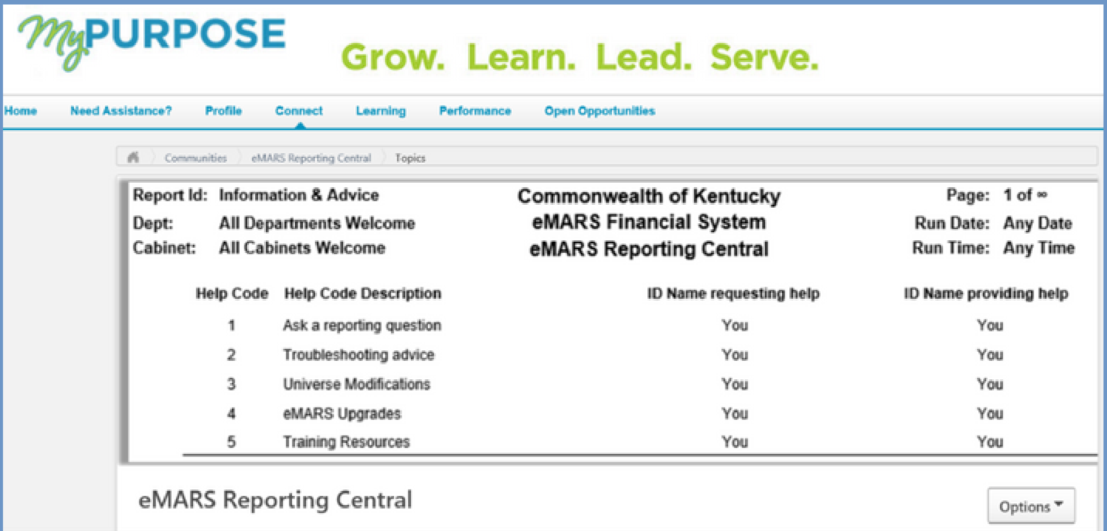
FORUM & TEAMS REMINDER
EMARS REPORT DEVELOPER COMMUNITY

Report developers are required to join the eMARS reporting discussion forum hosted on the MyPURPOSE platform. This forum is the primary vehicle for dispensing information to the developer community. The days of email blasts are over.

In addition to announcements, the forum is comprised of an expanding array of resources, including how-to guides, universe abstracts, universe modifications and additions, and statewide report query changes. It is also a centralized location for developers to collaborate and share development experience and knowledge.

There are currently several on-going projects discussed on the forum that will result in agencies potentially losing queries if not addressed.

Locate the MyPurpose icon on your desktop and select the *My*COMMUNITY option and join eMARS Reporting Central.



Report Id: Information & Advice
Dept: All Departments Welcome
Cabinet: All Cabinets Welcome

Commonwealth of Kentucky
eMARS Financial System
eMARS Reporting Central

Page: 1 of ∞
Run Date: Any Date
Run Time: Any Time

Help Code	Help Code Description	ID Name requesting help	ID Name providing help
1	Ask a reporting question	You	You
2	Troubleshooting advice	You	You
3	Universe Modifications	You	You
4	eMARS Upgrades	You	You
5	Training Resources	You	You

eMARS Reporting Central

If your agency is not able to access the MyPurpose/MyCommunity site, please contact the eMARS Reporting Lead at Dave.Sumner@ky.gov.

HELPFUL HINTS FROM CRC

eMARS Reporting Users:

We have been experiencing issues with certain web browsers when working in eMARS Reporting. Please try using **Mozilla Firefox** when working with eMARS Reporting.

If you use **Google Chrome**:

Please update your Chrome browsers to the latest version - 110.0.5481.100.

After the update, you will be able to refresh reports again in the 4.2 environments using Chrome.

Steps on how to update Chrome browser:

- Open Chrome browser
- Go to the top right, click on the three dots
- Select Help
- Select About
- The update will start immediately
- After the update, confirm you see version 110.0.5481.100
- Then close and reopen the browser
- Try to refresh a report and it should work

If you use **Microsoft Edge**, please update to the latest version - 110.0.1587.49.

Need access to eMARS, etc.?
Contact your Agency Security Lead

Need a vendor account created?
Contact your Agency Vendor Lead/Team

Need a document rejected in eMARS?
Contact your Approver

Looking for the Agency Delegation List?

These can all be found on the Finance Cabinet website, here.

HELPFUL HINTS FROM CRC

eMARS Agency Contacts:

The Office of the Controller uses Agency Delegated Contacts as the central point of contact for communications regarding eMARS and related issues. We also rely on each delegated agency contact to forward the information to all impacted users within their agency. It is imperative that agency contacts are correctly identified, and they disseminate eMARS communications to necessary users within their agency. Each agency has identified an Agency Implementation Lead (AILs) who is responsible for coordinating and monitoring efforts of the overall eMARS operation within their agency. To ensure we are communicating effectively, we are asking the AIL to review each contact identified on the Agency Delegated Contact list and provide updates as soon as possible.

A list of current agencies delegated contacts is available on the eMARS website. If contacts are incorrect, the Cabinet designee for the agency must complete the appropriate Agency Delegation and Contact Information Form and submit the updated packet to Marcia.Adams@ky.gov.

Additionally, the Office of Procurement Services maintains a separate, internal list of purchasing contacts. If you need to be informed of procurement-related issues and you are not on the purchasing contacts distribution list, please e-mail Shelby.Luby@ky.gov.

We greatly appreciate your cooperation and teamwork to ensure your users are informed timely.

PLEASE READ:

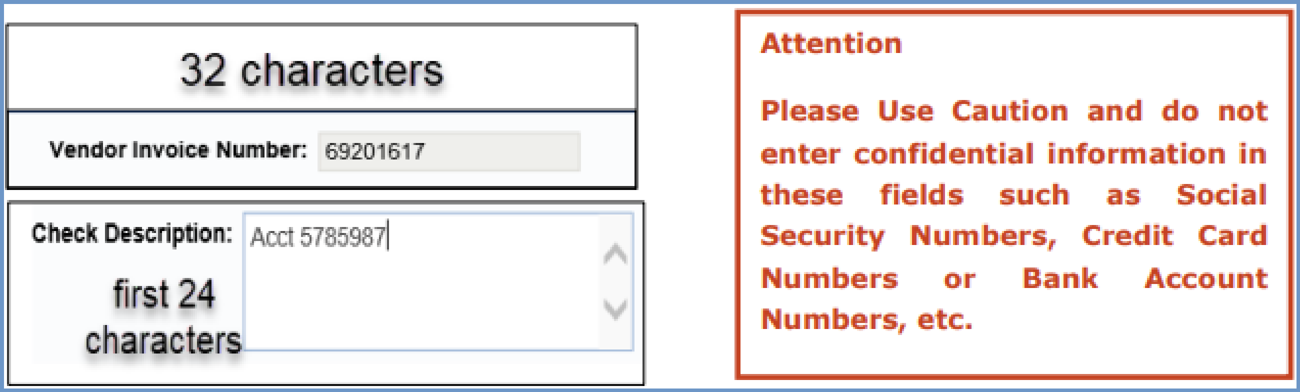
Payment Information, Checks, ACH, EFT, etc.:

The Customer Resource Center (CRC) Helpdesk receives hundreds of calls each month from vendors concerning checks (EFT/ACH and paper checks) and payments because they are not able to properly apply the payments into appropriate account. Vendors receiving payments must have adequate information to post payments correctly.

When making a payment, please add a detailed check description. This can include exactly what the payment is for, the actual invoice number, the account number, the agency. Do not use shorthand or acronyms. You might understand what it stands for but the vendor likely will not.

When processing a payment, there are two fields available to communicate proper allocation details to your vendors: Vendor Invoice Number (32 characters) and Check Description (first 24 characters). Both fields print on the check stub or in the ACH (EFT) email that goes out to vendors. In the case of ACH (EFT) vendors who are set up with a Disbursement Format of CTX, it is imperative that the proper information be included in the Vendor Invoice Number field.

Be sure to include the necessary identifying information, Invoice Number, Account Number, Case Number, Date of service, etc., in these two fields of your documents. Approvers should be looking for proper completion of these fields prior to approving the payment document.

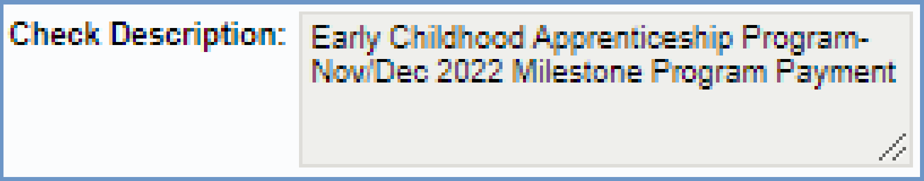


Vendor Invoice Number: 69201617

Check Description: Acct 5785987

Attention

Please Use Caution and do not enter confidential information in these fields such as Social Security Numbers, Credit Card Numbers or Bank Account Numbers, etc.



Check Description: Early Childhood Apprenticeship Program- Nov/Dec 2022 Milestone Program Payment