Public Fiduciary Department
Audit of Guardianship Services
By Maricopa County Internal Audit
November 2020

Why This Audit Is Important

The Maricopa County Public Fiduciary Department (MCPF) provides guardianship, conservatorship, and decedent services for vulnerable adults when no other person, agency, or corporation is qualified and willing to serve. Fiduciaries are licensed by the Arizona Supreme Court and regulated by the Administrative Office of the Courts.

We performed this audit to (1) assess MCPF's ward asset management process for ensuring ward assets are properly accounted for and managed, (2) review MCPF's oversight role of ward incurred expenditures, and (3) evaluate the adequacy of MCPF's information technology structure and protection of ward information.

Key Findings

- Ward asset management processes can be improved through more consistent account reconciliations and tracking.
- Additional internal controls and written procedures are needed for managing ward debit cards.
- Access controls can be strengthened for key software applications containing ward data.
- Contingency plans and procedures were enhanced and communicated to employees.

All key findings requiring corrective action were addressed through agreed-upon management action plans.

What We Audited

Following is a summary of work performed and findings. Corresponding recommendations and responses start on page 3. The responses were approved by Josephine Jones, MCPF Director, on October 12, 2020. More detailed observations and recommendations were communicated to management throughout the audit process.

Ward Asset Management

Background – To assess MCPF's ward asset management process, we interviewed key employees, reviewed applicable policies and procedures, and examined a sample of ward inventory accounts. Ward assets may include checking, savings, or investment accounts, insurance policies, or other assets valued over $99.

Observations – We found that ward inventory account reconciliations were not documented and that closed ward accounts are not always removed from the inventory account list

(**Recommendation 1**). Ward asset management policies are outdated and do not reflect current practices and desired internal controls (**Recommendation 2**). Inadequate ward asset management controls could result in mishandling of ward assets or non-compliance with statutory requirements.

Ward Expenditures

Background – MCPF is responsible for ensuring expenditures made by the wards are appropriate and authorized. To assess this oversight role, we interviewed key employees, evaluated policies and procedures, and reviewed processes for managing ward debit cards and monitoring usage.

Observations – We found that fiduciaries could order, receive, and deliver debit cards, set pin numbers, and perform card reconciliations on behalf of wards. Appropriate segregation of duties and procedures were not in place to help ensure that a fiduciary was not able to misuse a debit card. There were no written procedures for issuing and delivering ward debit cards (**Recommendation 3**). Establishing segregation of duties (e.g., having someone else perform the task of card delivery) and documenting procedures for card handling and reconciliation can help prevent and detect misuse of ward debit cards.

Information Technology Management

Background – MCPF relies heavily on various software applications for managing ward information. Some ward information is considered confidential. Properly restricting user access to the applications helps protect data and systems from loss or damage.

We interviewed key employees, reviewed supporting documentation, evaluated system settings, and tested a sample of user accounts to determine if access to five key MCPF software applications was adequately controlled. We evaluated controls over managing access requests and changes. We reviewed password requirements, remote access capabilities, segregation of duties, and IT security planning.

Observations – We found the following:

- Several user accounts had not been removed upon employee termination, change in job duties, or for accounts that were no longer in use (**Recommendation 4**).
- Security access levels within one key application (eGuardianship) lacked appropriate segregation of duties (**Recommendation 5**).
- Application limitations prevented MCPF from implementing password controls (e.g., length, complexity, unique to each user) that comply with County password requirements (**Recommendation 6**).
- Remote access to key applications is appropriately restricted to authorized employees.
- Policies and procedures have not been established for access management and related IT controls (**Recommendation 7**).

Contingency Planning

Background – Contingency planning helps ensure that critical information processing can be restored in the event of a disaster or unplanned interruption. Contingency planning often includes (1) a disaster recovery plan (DRP) that addresses restoring technology infrastructure and systems, and (2) a continuity of operations plan (COOP) that establishes policy and guidance to ensure critical business functions continue in the event of an emergency. MCPF relies on the Office of Enterprise Technology's DRP for restoring infrastructure and systems.

Observations – MCPF has prepared a draft COOP. We reviewed the draft and identified areas for improvement including updating contact information, establishing an alternate work site further away from MCPF, listing all IT equipment, and communicating with third-party vendors to gain assurances that critical backups are adequate to continue operations in the event of an unplanned outage (**Recommendation 8**). Contingency planning policies and procedures had not been established (**Recommendation 9**).

Additional Information

This audit was approved by the Maricopa County Board of Supervisors and was conducted in conformance with International Standards for the Professional Practice of Internal Auditing. This report is intended primarily for the County and its stakeholders. However, this report is a public record and its distribution is not limited. If you have any questions about this report, please contact Mike McGee, County Auditor, at 602-506-1585.

Recommendations and Responses

Recommendations	Responses
1 Ensure account statements are reviewed and reconciliations are performed and documented for all ward funds held in individual ward accounts.	Concur – in progress Implementation Plan: 1. Continue to review and reconcile all financial accounts for MCPF wards upon receipt of statements. 2. Retain bank statements in a uniformed manner within MCPF filing system. 3. Develop tracking system to ensure bank accounts are built on the individual client's inventory tab, statements are reviewed regularly, and values are updated at regular intervals. Target Date: 3/30/2021

Recommendations	Responses
2 Update ward asset policies and procedures to ensure they reflect current practices and desired internal controls.	Concur – in progress Implementation Plan: 1. Update MCPF Policy E-09 to reflect current practice. 2. Establish schedule to perform quarterly internal audits of all managed client assets, including valuations. 3. Reconcile client financial accounts upon receipt of account statement. 4. Retain all supporting documentation within MCPF's filing systems according to record retention guidelines. Target Date: 2/28/2021
3 Establish written debit card procedures that address: • Proper segregation of duties throughout the debit card process • Capturing key information for issuing and distributing ward debit cards (e.g., request, approval, receipt, pin, delivered) • Reconciliation of monthly debit card statements • Deactivation of continually unused debit cards • Retention of supporting documentation	Concur – in progress Implementation Plan: 1. Add debit card procedures to MCPF Policy #E-01 and outline the process and duties of key personnel, ensuring segregation of duties is demonstrated, including monetary spending limits, deliver, reconciliation of statements, and handling of active and inactive debit cards. 2. Formalize office policy to include requirement that a justification memo be completed and approved for any unusual expenditure over $500 (excluding standard payments for share of cost, mortgage, rent, insurance premiums, etc.). 3. Add additional layer of approval on SharePoint form for new debit card requests to require supervisor review prior to establishing new debit cards. Target Date: 01/31/2021
4 Remove user access to key applications for non-current MCPF employees.	Concur – in progress Implementation Plan: Complete review of all access users and submit OET ticket to remove accounts that should already be removed/modified. Target Date: 12/31/2020

Recommendations	Responses
5 Review and update current access levels within eGuardianship and ensure that users' permission rights are necessary for their job duties.	Concur – will implement with modifications Implementation Plan: 1. Review User Guide and develop written descriptions that correlate with job duties that support user access levels. 2. Implement periodic review of eGuardianship access levels by designated staff to ensure security access levels are sufficient to allow staff to perform job duties as assigned. Target Date: 1/31/2021
6 Ensure passwords for key applications meet minimum strength requirements. Where application limitations exist, establish policy addressing password requirements including password strength, confidentiality, and uniqueness to each user.	Concur – will implement with modifications – Management accepts the risk of this issue. Implementation Plan: 1. Establish a procedure for key systems password management and requirements for new and active employees, emphasizing password confidentiality and strengths. 2. Work towards automation of passwords and periodic password renewals. 3. Work with systems to create password requirements that are controlled by the employee, where applicable. MCPF will accept risk on those systems that do not allow modifications. 4. Include password application requirements in any new RFP for new office banking/case management software. Target Date: 1/31/2021
7 Establish written user access policies and procedures to address user access approval, removal, reviews, password requirements, remote access, segregation of duties, and IT security training.	Concur – in progress Implementation Plan: 1. Develop User Access Guide for all programs 2. Implement "Security Forms" requiring signature approval for each security setting. Target Date: 1/15/2021

Recommendations	Responses
8 Complete the MCPF continuity of operations plan (COOP).	Concur – completed Implementation Plan: 1. MCPF COOP generated using the MaricaopRegionPrepares.com planning website. Contact information updated within the online living plan. 2. Virtual meeting with eGuardianship on 10/15/20 to track status of vendor updates including description of how information is backed-up and frequency of backup. 3. Create process training document for fiduciaries to routinely save/print caseload repot to have list of wards and contact information. 4. COOP training in development. 5. MCPF COOP signed off by Director Lina Garcia on March 3, 2020. 6. Training to be scheduled for November 2020 at which time COOP will be disseminated to MCPF staff. Target Date: This recommendation was implemented by the department prior to report issuance.
9 Establish policy and procedures to ensure the COOP is regularly reviewed, updated, tested, and communicated to MCPF employees.	Concur – completed Implementation Plan: Will draft process documenting procedures in place to ensure COOP is reviewed, updated, tested, and communicated to MCPF employees. Target Date: This recommendation was implemented by the department prior to report issuance.