03/24/2025

Electronic Funds Transfer (EFT) Fraud Scheme

Background:

The U.S Department of Health and Human Services, Office of the Inspector General (HHS-OIG) has issued an alert and report on electronic funds transfer (EFT) fraud schemes re-routing Medicare and Medicaid provider payments to fraudulent accounts.

Key Details:

This notice is to inform MCOs of the EFT fraud scheme targeting various state's Medicaid systems and redirecting payments to providers. HHSC is providing MCOs the HHS-OIG fraud alert notice and the report of survey findings on the impacts of this scheme and its recommendations to mitigate EFT fraud. HHSC also encourages MCOs to share this information with their providers as appropriate.

Resources:

HHS-OIG EFT Fraud Scheme Alert (attached)

HHS-OIG EFT Fraud Survey Report (attached)

Contact:

MCCO Monitoring Team

Attachment:

HHS-OIG EFT Fraud Scheme Alert.pdf HHS-OIG EFT Fraud Survey Report.pdf

Type: Informational

To: CHIP; CMDS; DMO; MMP; STAR; STAR+PLUS; STARHEALTH; STAR_KIDS

From: MCCO

HHS-OIG Fraud Scheme Alert

The U.S. Department of Health and Human Services, Office of the Inspector General (HHS-OIG), in cooperation with other law enforcement partners, is notifying payers about high-risk requests to re-route electronic funds transfers (EFTs) to fraudulent accounts owned by cybercriminals. State Medicaid agencies have been targeted, and an HFPP Partner noted that fraudulent EFT forms were transmitted to Medicaid to redirect funds from an institutional provider. Private sector payers have also been targeted, but currently there are no losses reported.

Partners receiving high-risk requests should:

- Confirm the requestor's identity using information on file, not what was provided in the request.
- Refrain from providing financial or sensitive information over the phone or through email.
- Contact your HFPP Partner Liaison to be connected to the law enforcement agency investigating this scheme.

Department of Health and Human Services

Office of Inspector General

Office of Evaluation and Inspections

March 2025 | OEI-07-23-00180

Medicare and Medicaid Payments to Providers Are at Risk of Diversion Through Electronic Funds Transfer Fraud Schemes

March 2025 | OEI-07-23-00180

Medicare and Medicaid Payments to Providers Are at Risk of Diversion Through Electronic Funds Transfer Fraud Schemes

Why OIG Did This Review

- OIG identified a fraud scheme in which fraudsters diverted Federal and State payments intended for providers. Specifically, individuals purporting to be hospital providers have targeted the Medicare and Medicaid programs by submitting fraudulent electronic funds transfer authorization requests or other schemes to divert payments for providers to fraudsters.
- There is a potential for large losses associated with electronic funds transfer fraud, given how widely electronic funds transfer transactions are used within the health care industry. Recently, fraudsters who were able to gain unauthorized access to email accounts targeted the HHS grant Payment Management System, leading to millions of dollars in losses in 2023.

What OIG Found

Two-thirds of surveyed entities that process payments for Medicare and Medicaid (i.e., payors) reported that they were aware of being targeted by electronic funds transfer fraud schemes, some of which were frequent or recurring.

Medicare and Medicaid payors most frequently reported using verified communication channels or knowledge-based methods to confirm electronic funds transfer changes.

Some Medicare and Medicaid payors described employing security measures that align with recommendations from expert groups.

CMS took steps to mitigate threats from electronic funds transfer fraud schemes in Medicare.

Nearly three-fifths of surveyed Medicare and Medicaid payors expressed interest in implementing additional measures to mitigate electronic funds transfer fraud threats, but some reported challenges or barriers to implementation.

What OIG Recommends

OIG recommends that CMS:

1. Engage Medicare Administrative Contractors on improving security measures.
2. Share information with State Medicaid agencies to help improve security measures.
3. Support periodic information sharing to mitigate evolving threats of electronic funds transfer fraud schemes.

CMS did not explicitly state its concurrence or nonconcurrence with the first two recommendations as initially drafted; OIG has altered these recommendations slightly to clarify OIG's intent. CMS did not concur with the third recommendation.

TABLE OF CONTENTS

BACKGROUND

OBJECTIVES

1. To identify the extent to which entities that process payments for Medicare and Medicaid (i.e., payors) reported experiencing being targeted by fraudulent electronic funds transfer (EFT) requests.
2. To identify practices that CMS and Medicare and Medicaid payors reported employing to reduce EFT fraud.
3. To assess what additional measures, if any, could be taken to mitigate risks of EFT fraud.

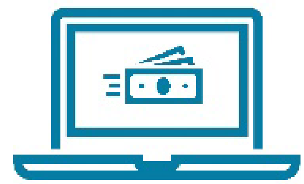
Between 2020 and 2022, an emerging fraud scheme targeted at least 4 Medicare Administrative Contractors and 22 State Medicaid agencies.[1, 2] Individuals purporting to represent hospital providers targeted the Medicare and Medicaid programs by submitting fraudulent EFT authorization requests to these agencies. Some of these agencies updated hospital providers' bank account information to reflect the accounts specified on the fraudsters' requests, causing claims payments intended for providers to be diverted to fraudulent accounts. Thus far, these types of fraud schemes targeting hospital providers have resulted in reported diversion of approximately $26.5 million from the Medicare and Medicaid programs (see Appendix A for information on EFT fraud cases investigated by OIG). More recently, fraudsters who were able to gain unauthorized access to email accounts carried out a scheme that targeted the HHS grant Payment Management System, leading to millions of dollars in losses in 2023.[3]

There is a potential for large losses associated with EFT fraud schemes in health care (see Exhibit 1 for information on common threats). In the Medicare program alone, the Centers for Medicare and Medicaid Services (CMS) and its contractors process over one billion claims annually and 2023 expenditures were more than $1 trillion. Medicare requires providers that enroll in the program to agree to receive claims payments via EFT, and most Medicaid providers are also paid by State Medicaid agencies via EFT.[4, 5]

Exhibit 1: Primer on Electronic Funds Transfers, Related Fraud Threats, and Recommended Security Measures to Protect Against Fraud

Electronic Funds Transfers

- **Electronic Funds Transfer (EFT):** EFT transactions are used to transmit payments from a payor to a bank account (e.g., direct deposit).
- **EFT Authorization:** The process of an account holder enrolling to receive payments via EFT transactions.
- **EFT Change:** The process of an account holder updating their EFT enrollment information (e.g., requesting changes to account or bank information).



EFT Fraud Threats

- **EFT Fraud:** EFT fraud occurs when fraudsters divert payments from the intended recipient to an unauthorized account. Expert groups have highlighted several security threats that could present opportunities for EFT fraud schemes, including:

Phishing Attacks: Attacks in which individuals are lured (e.g., through deceptive emails) into disclosing to a bad actor sensitive information such as credentials or a password that could be used to facilitate an EFT fraud scheme. A phishing attack could serve as a precursor to an impersonation attack.

Impersonation Attacks: Attacks in which fraudsters use falsified identity documentation or stolen information to claim an account holder's identity or pose as an authorized individual associated with an account to make account changes.

Insider Threats: Threats that insiders (e.g., a representative within an organization) will use their authorized access to perpetrate or facilitate EFT fraud. Opportunities for EFT fraud can include accidental insider threats, a subset of insider threats, which may occur when insiders lack awareness of applicable security policies or make procedural errors that enable EFT fraud to occur.

Recommended Security Measures to Protect Against Threats Including EFT Fraud

Expert groups have recommended a variety of measures to promote security and mitigate schemes such as those used to commit EFT fraud. Expert groups referred to in this report include the National Institute of Standards and Technology (NIST); the HHS Healthcare and Public Health Sector Coordinating Council; the Federal Financial Institutions Examination Council; and the Workgroup for Electronic Data Interchange.

- **Layered Security:** Expert groups recommend employing layered security, which incorporates multiple preventative, detective, and corrective controls, and is designed to compensate for potential weaknesses in any one control. Individual measures that could be included in layered security include:

  - **Multifactor Authentication:** The use of more than one distinct authentication factor for successful authentication. There are three types of authentication factors:

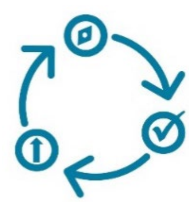
Something you **know** (e.g., a password that could be entered to log into a secure portal, a PIN, or knowledge-based questions regarding recent transactional history);

Something you **have** (e.g., a smart card; an identifiable device such as a mobile phone; or a confirmed communication channel such as an address or phone number of record); and

Something you **are** (e.g., a biometric characteristic).

  - **Fraud Detection Measures:** The use of measures such as transaction logs or monitoring processes to help identify and/or alert entities to unauthorized activities or suspicious behaviors.
  - **Systemic Security Controls:** Safeguards or countermeasures within a system to manage security risks by limiting account access, activities, and privileges.
  - **Training and Education:** Educating providers and pertinent staff to increase awareness of fraud risks and effective techniques to mitigate the risks.

- **Information Sharing:** Expert groups recommend information-sharing programs to help pool expertise on security measures across multiple organizations. This can help participating organizations learn about novel attacks and mitigation strategies before their organization is targeted. Information sharing can also help support continuous innovation across organizations in response to evolving challenges and best practices.



- **Continuous Monitoring and Assessment:** Expert groups recommend continuous monitoring at the system level to facilitate ongoing assessments of system security and to support organizational risk management decisions.

Electronic Funds Transfers

EFT transactions are used within the health care industry to transmit payments from a health plan to a provider's bank account. Standards for these types of transactions were established pursuant to the Health Insurance Portability and Accountability Act[6] and the Patient Protection and Affordable Care Act,[7] the latter of which mandated the adoption of operating rules for health plan EFTs.

The HHS Secretary by regulation[8] adopted the Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) rules as operating rules for health care EFTs.[9, 10] The rules specify information that must be included in the transactions and set limits on the data elements that a health plan may request from a provider for EFT enrollment.

EFTs in Medicare and Medicaid

Medicare Parts A/B. All providers that enroll in Parts A and B of the Medicare program must agree to receive Medicare payments by EFT.[11] Providers enrolling in Medicare or updating their existing EFT information must submit an EFT authorization agreement to the applicable Medicare Administrative Contractor or through the Medicare Provider Enrollment, Chain, and Ownership System (PECOS). Medicare Administrative Contractors are responsible for reviewing these requests and entering all EFT data into PECOS.

CMS guidance contains information on payments to provider bank accounts and requirements for processing and verifying EFT authorizations[12] in the Medicare program.[13, 14] The guidance notes that Medicare Administrative Contractors should review a voided check or a bank letter to verify account information on EFT authorizations and should contact the provider or an authorized official to verify EFT changes.

Medicaid and Medicaid Managed Care Organizations. Although each State Medicaid agency must comply with Federally mandated operating rules for EFT enrollment data, there is no national enrollment database for Medicaid-only providers[15] and no standard process for EFT enrollment in Medicaid. Each State Medicaid agency has its own screening, enrollment, and EFT authorization and change processes. State Medicaid agencies that seek to enhance EFT processes or security functions within their State claims processing and program administration information systems may be eligible for Federal matching funds.[16]

In many States, State Medicaid agencies contract with Medicaid MCOs to administer some or all Medicaid services, and enrolled providers receive payments through Medicaid MCOs or their contracted entities. Like State Medicaid agencies, Medicaid MCOs have their own EFT requirements and authorization processes.

Related Work

OIG has completed prior work to advise HHS leaders on maintaining effective security measures (e.g., systemic security controls) when implementing new information systems, and to alert CMS about vulnerabilities related to provider payments and inaccuracies in provider data contained in CMS systems.[17, 18, 19] Security vulnerabilities and inaccurate or outdated information in CMS systems could present opportunities for bad actors to commit fraud when submitting EFT authorization or change requests. In 2009, OIG made recommendations to CMS to revalidate provider enrollment information and update PECOS.[20] In response to recommendations in the report, CMS took actions including revalidating Medicare provider information in CMS systems and educating providers on reporting responsibilities and the need to update their enrollment information.

Methodology

Scope

We designed this evaluation to gather insights into the potential scope of EFT fraud and vulnerabilities to EFT fraud in Medicare and Medicaid, having been alerted to a potential fraud trend by OIG investigators. To collect general information on the scope, monetary impact, and potential ongoing vulnerabilities to EFT fraud in Medicare and Medicaid, we conducted a nationwide review between June and October 2023. We surveyed Medicare (Parts A and B) and Medicaid payors or their designees that process payments to providers.[21] We directed payors to respond for the timeframe of January 2020 to June 2023.

This work did not estimate the amount of EFT fraud that occurred or quantify the extent to which payors' reported validation measures reduced fraud. Further, this evaluation was not designed as a test of CMS or Medicare and Medicaid payors' protections against EFT fraud or whether payors' security measures were compliant with Federal regulations, to the extent they exist, or met best practices established by expert groups.

Data Sources and Analysis

We surveyed Medicare (Parts A and B) and Medicaid entities or their designees that process payments to providers. To gather information from Medicare payors, we surveyed the 7 Medicare Administrative Contractors operating across all 12 Medicare A/B jurisdictions. To gather information from Medicaid payors, we surveyed all 51 State Medicaid agencies (including the District of Columbia) and all 5 U.S. Territorial Medicaid agencies. We also selected 13 Medicaid MCO parent companies on the basis of number of enrollees.[22]

We also asked payors to provide documentation of the forms or systems each payor used to process provider EFT enrollments and changes in EFT bank account information. Our review of these materials did not provide additional insights beyond the survey responses; therefore, this information was not included in our findings. In addition, we asked CMS about its efforts to help mitigate EFT fraud in Medicare and Medicaid.

The survey to Medicare and Medicaid payors included closed- and open-ended questions covering EFT authorization and change processes; EFT validation measures; and payors' experiences with EFT fraud schemes. The survey also asked payors for their insights about the extent to which they would like to take additional measures to mitigate their risks of EFT fraud and any barriers they anticipated to implementing additional protections. Survey questions regarding validation measures for EFT authorization and change processes reflected some, but not all, recommendations from expert groups to promote security and mitigate schemes such as those used to commit EFT fraud. Expert groups referred to in this report include the National Institute of Standards and Technology (NIST); the HHS Healthcare and Public Health Sector Coordinating Council; the Federal Financial Institutions Examination Council; and the Workgroup for Electronic Data Interchange.

Our survey response rate was 100 percent. We analyzed responses to closed-ended questions and conducted a thematic review of qualitative data. On the basis of this review, we identified the most salient takeaways and followed up with select payors to collect additional details.

We also collected case information from OIG investigators on recent criminal sentencings in EFT fraud cases they investigated to identify sentences, restitution amounts, and victims in Medicare and Medicaid (see Appendix A).

Limitations

This evaluation relies on self-reported survey data. We did not independently verify payors' experiences and responses regarding EFT processes and fraud schemes. Further, payors varied in the amount of detail they provided in open-ended survey responses.

The reporting of fraud schemes can vary on the basis of the sophistication of payors' detection mechanisms; therefore, there may have been other incidents that went undetected and therefore unreported.

Standards

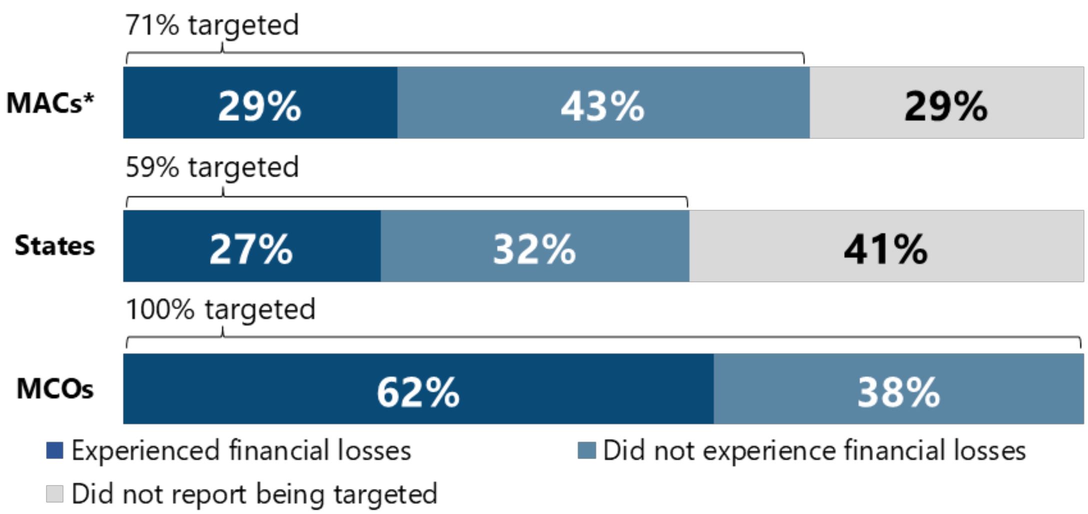
We conducted this study in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

FINDINGS

Two-thirds of surveyed Medicare and Medicaid payors reported that they were aware of being targeted by EFT fraud schemes, some of which were frequent or recurring

Among surveyed Medicare Administrative Contractors, State Medicaid agencies, and Medicaid MCOs, 67 percent reported they had been targeted by EFT fraud schemes. Further, half of the targeted payors reported that they experienced financial losses from EFT fraud. Of the payors that reported being targeted by EFT fraud, Medicare Administrative Contractors and State Medicaid agencies were less likely to report experiencing financial losses relative to Medicaid MCOs (see Exhibit 2).

Exhibit 2: A majority of Medicare and Medicaid payors reported being targeted by EFT fraud, but this did not always result in financial losses.



* Note: Medicare Administrative Contractor percentages do not add to 100 because of rounding.
Source: OIG analysis of payor survey data from 7 A/B Medicare Administrative Contractors (MACs), 56 State Medicaid agencies (States), and 13 Medicaid MCO parent companies (MCOs), 2024.

Payors that reported they were targeted by EFT fraud described varied and sophisticated schemes involving phishing attempts, impersonation attacks, and insider threats. In response to open-ended survey questions, payors reported phishing schemes in which fraudsters sent emails imitating legitimate accounts or from compromised business email accounts. Other payors described EFT fraud schemes tied to impersonation attacks, such as a bad actor leveraging employee identity information to make EFT changes. Payors also reported experiencing EFT fraud after non-authorized individuals were able to make EFT changes over the phone or through a provider portal. Although some of these payors were able to identify fraud schemes quickly and prevent payments from being lost to fraud, other schemes ultimately resulted in financial losses.

Medicare and Medicaid payors that reported they were targeted and ultimately experienced financial losses from EFT fraud reported loss amounts ranging from $140,000 to $1 million. One Medicare Administrative Contractor reported a loss of $434,000 from the Medicare trust fund; they attributed the loss to an impersonation scheme. A State Medicaid agency reported experiencing financial losses in early 2020, noting that "a half-dozen or so fraudulent payments were made amounting to a total of about $1 million before the issues were corrected." Additionally, a Medicaid MCO reported experiencing EFT fraud related to both Medicare and Medicaid EFT enrollment accounts.[23] The Medicaid MCO indicated that the combined losses associated with these fraud incidents totaled approximately $500,000.

Sixteen Medicare and Medicaid payors reported experiencing multiple, frequent, or ongoing threats from EFT fraud schemes

Of those that reported being targeted by EFT fraud, 16 payors (1 Medicare Administrative Contractor, 9 State Medicaid agencies, and 6 Medicaid MCOs) indicated in response to open-ended questions that they had experienced multiple, frequent, or ongoing fraud attempts.[a] These 16 payors were responsible for processing Medicare and/or Medicaid claims for approximately 20 million enrollees in 36 States. Although the frequency of these attempts varied, some of these payors described experiencing numerous fraudulent requests each week; other payors reported experiencing up to 20 to 25 incidents of attempted EFT fraud between 2021 and 2023. Payors reported that these requests often contained detailed information needed for account verification.

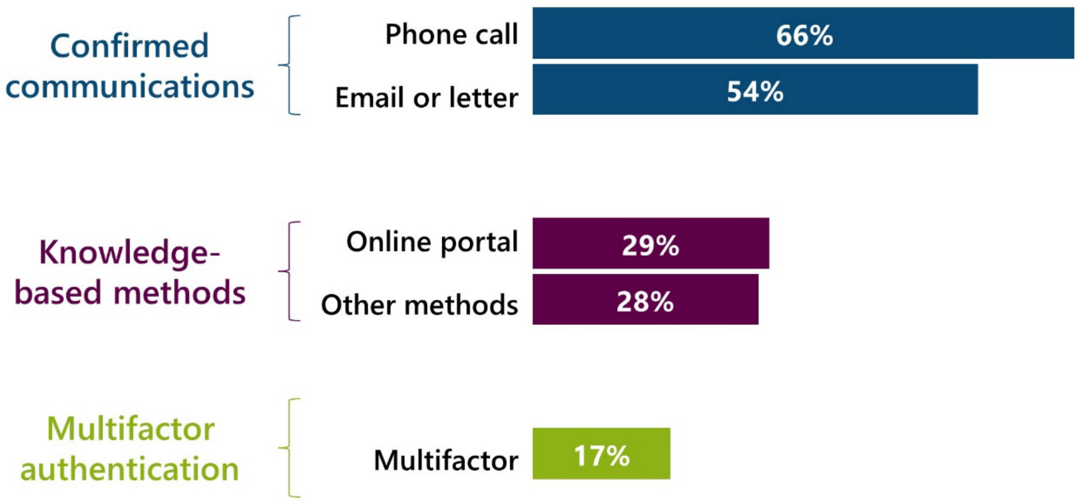
Medicare and Medicaid payors most frequently reported using verified communication channels or knowledge-based methods to confirm EFT changes

Payors most frequently reported using security measures including contacting authorized individuals through confirmed communication channels (e.g., calling, emailing, or mailing a letter to a designated point of contact) or using knowledge-based methods such as password-protected provider portals. Few Medicare and Medicaid payors reported using multifactor authentication. Specifically, just under one-fifth of State Medicaid agencies, just under one-quarter of Medicaid MCOs, and no Medicare Administrative Contractors reported employing multifactor authentication.[24]

[a] OIG captured payors' reported experiences with EFT fraud via open-ended survey questions and analyzed their responses for themes and insights. We can quantify how many payors *reported* multiple, frequent, or ongoing threats from EFT fraud schemes, but not how many payors *experienced* multiple, frequent, or ongoing threats.

See Appendix B for detailed results from our survey's closed-ended questions.

Exhibit 3: Medicare and Medicaid payors most often reported employing validation or notification measures including confirmed communication channels and knowledge-based methods.



Source: OIG analysis of payor survey data from 7 A/B Medicare Administrative Contractors, 56 State Medicaid agencies, and 13 Medicaid MCO parent companies, 2024.

All Medicare and some Medicaid payors reported using phone calls or other communication channels to notify payors of EFT change requests

Overall, two-thirds of payors, including all Medicare Administrative Contractors, reported that they conduct a phone call with a designated point of contact regarding EFT changes.[25] Placing a phone call with a designated point of contact could help a payor confirm that requested EFT changes are valid. However, more than one-third of State Medicaid agencies and two-fifths of Medicaid MCOs did not report employing a phone call.

Medicare and Medicaid payors also reported using other communication channels such as emails or letters to designated contacts on file to notify them of requested changes to EFT information.[26] Specifically, more than two-thirds of Medicare Administrative Contractor and Medicaid MCO payors reported employing emails or letters, but fewer than half of State Medicaid agencies did so.

Some Medicare and Medicaid payors reported using knowledge-based validation methods to help secure EFT processes, such as online provider portals or security questions

Overall, more than two-fifths of payors reported employing knowledge-based validation methods to confirm EFT changes. Knowledge-based validation methods include the use of passwords (e.g., a password-protected provider portal), PINs, or security questions that help to validate the identities of providers requesting EFT changes.

A little more than one quarter of Medicaid payors reported that they require providers to submit EFT information via an online provider portal. An online portal provides a password-secured process (i.e., requiring knowledge-based verification) for submitting EFT information. However, all Medicare Administrative Contractors, more than two-thirds of State Medicaid agencies, and more than half of Medicaid MCOs reported allowing providers to submit EFT authorization and change requests via paper forms, rather than requiring all providers to use an online portal. The use of paper forms could reduce payors' abilities to limit access to EFT processes behind a secure provider portal.

More than one-quarter of Medicare and Medicaid payors reported using other knowledge-based verification methods (e.g., requiring providers to verify their identity using a previously issued PIN or by answering questions regarding recent transactions). Specifically, just over half of Medicare Administrative Contractors, less than one-quarter of State Medicaid agencies, and just under one-third of Medicaid MCOs employed these types of knowledge-based measures.

Some Medicare and Medicaid payors described employing security measures that align with recommendations from expert groups

In response to open-ended questions requesting that they describe their validation processes and security measures, some payors described employing practices such as systemic security and fraud detection measures.[27] We found that 26 Medicare and Medicaid payors reported employing systemic security measures to help mitigate risks associated with EFT authorization and change processes. These payors reported using measures such as enforcing account roles and permissions, and sending paper checks temporarily to a confirmed address of record after EFT changes are submitted. Additionally, 11 Medicare and Medicaid payors reported using fraud detection measures to help assess the security of their processes or to identify suspicious activities. For example, one Medicaid MCO reported monitoring accounts for suspicious activity, ongoing trends, patterns, and metrics.

Expert groups emphasize that using multiple types of controls as part of layered security is important to help ensure that the inherent vulnerabilities of any single measure are compensated for by other measures (see Exhibit 1). Thus, combining multiple controls such as multifactor authentication, account access restrictions, and fraud detection measures could help payors present a layered security posture to mitigate threats of EFT fraud.

CMS took steps to mitigate threats from EFT fraud schemes in Medicare

CMS reported that it took steps to mitigate EFT fraud in the Medicare program by securing provider enrollment systems and issuing updated guidance for Medicare Administrative Contractors related to EFT verification. Specifically, CMS reported implementing multifactor authentication for provider enrollment systems, including its access management system (IDM)[28] and PECOS, where providers or Medicare Administrative Contractors may enter or update provider EFT data.[29] Strengthening security for these systems could help CMS and Medicare Administrative Contractors ensure that unauthorized individuals are not able to gain access to or change payment information stored in systems such as PECOS. However, CMS noted that improvements to PECOS can only be consistently leveraged to support identity authentication and reduce EFT fraud in the Medicare program. CMS reported that State Medicaid agencies have limited abilities to leverage PECOS data to reduce EFT fraud and Medicaid MCOs do not have access to PECOS. CMS took other steps to support EFT verification in the Medicare program by issuing nonpublic guidance for Medicare Administrative Contractors in 2021 and 2024 that outlined updated EFT procedures.

Medicare Administrative Contractors reported coordinating or communicating with CMS and other Medicare Administrative Contractors to mitigate recurring EFT fraud

In response to open-ended questions, payors reported that when an EFT fraud scheme targeted multiple Medicare Administrative Contractors, several of these payors reported coordinating with CMS and other Medicare Administrative Contractors to mitigate further EFT fraud attempts. In one case, a payor described receiving a fraud alert, implementing protective measures based on CMS's updated EFT verification guidance, and conducting a review of recent EFT change requests to identify suspicious activities. Through this review, the Medicare Administrative Contractor identified a potentially fraudulent application and worked with CMS to resolve the issue. Five other payors reported engaging with CMS and/or other Medicare Administrative Contractors on topics including EFT verification procedures, best practices when reviewing EFT submissions, and validation services to counter EFT fraud. These engagements align with recommendations from expert groups that have highlighted the importance of regular information-sharing programs for organizations to share expertise, learn about novel attacks others are facing, and stay apprised of security threats including evolving EFT fraud schemes.

Nearly three-fifths of surveyed Medicare and Medicaid payors expressed interest in implementing additional measures to mitigate EFT fraud threats, but some reported challenges or barriers to implementation

Whether surveyed payors reported being targeted by EFT fraud or not, many expressed interest in implementing additional measures to mitigate their vulnerabilities to EFT fraud schemes. In response to a closed-ended question, nearly three-fifths of payors reported they were interested in implementing additional validation processes or security measures to guard against EFT fraud. Some of these payors that reported interest in implementing additional security measures also described the types of measures they would be interested in implementing. In response to open-ended questions, these payors expressed interest in implementing technological improvements or sharing information with other agencies to help strengthen protections against EFT fraud.[b]

Medicaid payors expressed interest in technology enhancements to help validate provider identities. In response to open-ended questions, 15 State Medicaid agencies and Medicaid MCOs reported that they had interest in enhancing their abilities to validate providers' identities through technologies such as biometric identification, processes to identify devices, or implementing multifactor authentication methods. For example, one State Medicaid Agency noted that it was in the process of implementing a new provider portal and reported interest in multifactor authentication to verify providers' identities. Five Medicaid MCOs expressed interest in technologies including device fingerprinting and biometric security measures.

Medicaid payors expressed interest in sharing information and learning about measures to reduce fraud. In response to open-ended questions, 12 State Medicaid agencies and Medicaid MCOs expressed interest in information sharing, partnerships, or learning about best practices, which could help Medicaid payors strengthen their protections against threats of EFT fraud. Some State Medicaid agencies expressed uncertainties regarding available measures to mitigate EFT fraud, and information sharing could help these payors—as well as others with less robust security practices—learn about measures used by other payors with stronger protections in place. Further, one State Medicaid agency reported interest in an alert system to notify others when a payor experiences an EFT fraud attempt, which could help all payors stay apprised of evolving EFT fraud schemes. Medicaid MCOs

[b] OIG captured payors' interest in implementing technology enhancements or sharing information via open-ended survey questions and analyzed their responses for themes and insights. We can quantify how many payors *reported* they had interest in technology enhancements or information sharing, but this may not capture all payors who may have had *interest* in implementing technology enhancements or sharing information.

expressed interest in enhancing partnerships in the industry, which could serve as another way for payors to learn about emerging EFT threats.

One-third of Medicare and Medicaid payors reported experiencing challenges or barriers implementing new processes or measures

We found that one-third of surveyed Medicare and Medicaid payors indicated that they had encountered challenges or barriers implementing new security measures to reduce opportunities for EFT fraud. These included challenges contacting providers to validate EFT changes and challenges meeting the financial and staffing requirements associated with some validation methods, as well as barriers presented by the real or perceived burdens placed on providers by some validation methods.

Operational challenges may have hindered Medicare and Medicaid payors from implementing protections against EFT fraud. In response to open-ended survey questions, payors reported several operational challenges to implementing new EFT enrollment or change processes, including difficulties related to inaccurate provider contact information.[c] Seven Medicare and Medicaid payors reported challenges contacting providers or their designated contacts to validate EFT changes, in part because the providers' contact information was not always current in the payors' data systems. For example, one State Medicaid agency reported that although its practice was to contact the authorized representative on the provider's record rather than the individual submitting the EFT change request, the authorized representative on file may no longer be valid, or their contact information may have changed. Another State Medicaid agency reported that the need to maintain current provider contact information can serve as a barrier to implementing additional protections against EFT fraud because keeping this information updated requires action by providers. Additionally, Medicaid payors noted that the costs and staffing needs associated with some validation methods prohibited them from implementing new protections against EFT fraud.

Medicaid payors reported barriers related to provider burden that may have also hindered the implementation of protections against EFT fraud. Medicaid payors also reported barriers related to provider burden regarding new validation methods, which served as a barrier to instituting additional security measures. In response to an open-ended survey question on barriers, three Medicaid payors reported that providers were uncomfortable sharing additional confidential information as part of enhanced validation processes. Other Medicaid payors reported that providers expressed frustration with additional security measures that extended the processing time to update providers' EFT information. To reduce the barriers presented by the real or perceived provider burden associated with new EFT

[c] OIG captured payors' responses regarding challenges or barriers in open-ended survey questions and analyzed their responses for themes and insights. We can quantify how many payors *reported* operational challenges or barriers, not how many payors *experienced* operational challenges or barriers.

fraud mitigation measures, provider education could prove beneficial. Expert groups recommend educational programs to help increase awareness of fraud risks and educate providers and staff on effective techniques to mitigate the risks.

CONCLUSION AND RECOMMENDATIONS

EFT fraud attempts are widespread and dynamic. Roughly one-third of surveyed Medicare Administrative Contractors (Parts A/B), State Medicaid agencies, and Medicaid MCOs reported experiencing financial losses due to EFT fraud, with loss amounts ranging from $140,000 to $1 million. The full extent of EFT fraud could be more extensive, as measuring the threat can depend on the sophistication of payors' detection mechanisms. Given the amount of money flowing through Medicare and Medicaid, there is a potential for continued financial risk associated with EFT fraud. The recent diversion of funds from the HHS grant Payment Management System emphasizes the harmful nature of these kinds of schemes, with that incident leading to millions of dollars in losses in 2023.

Most Medicare and Medicaid payors have some validation methods in place, and CMS has taken some steps to address EFT fraud in Medicare. However, the risks OIG identified warrant further action to protect Federal funds, and many payors expressed interest in implementing additional security measures to mitigate evolving EFT fraud threats. We offer the recommendations below as means to assist Medicare and Medicaid payors in making specific payment systems upgrades and procedural changes to help address this fraud risk.

We recommend that CMS take the following actions:

Engage Medicare Administrative Contractors regarding opportunities and barriers to improving security measures for EFTs that were reported in response to OIG's survey

To support program integrity and advance protections to mitigate evolving EFT fraud threats, CMS should continue its technical assistance efforts in the Medicare program and further those efforts by considering additional measures identified via OIG's survey. Specifically, CMS should engage Medicare Administrative Contractors regarding the implementation of further security measures and barriers in addition to implementing new measures that some Medicare Administrative Contractors reported in survey responses. If appropriate, CMS could consider offering technical assistance to Medicare Administrative Contractors regarding opportunities and barriers identified via the survey and through this engagement. After issuing this report, OIG will provide CMS with pertinent Medicare Administrative Contractor survey responses.

Share information with State Medicaid agencies to help address challenges implementing security measures to protect against EFT fraud

To support program integrity and advance protections to mitigate evolving EFT fraud threats in Medicaid, CMS should build upon its prior efforts to mitigate EFT fraud in the Medicare program. Specifically, CMS should support State Medicaid agencies in protecting against EFT fraud by sharing information on security improvements for EFTs and the availability of matching funds for these improvements.

This could include presenting an information session or issuing an informational memorandum on recent improvements to CMS systems (i.e., IDM and PECOS) and EFT guidance offered to Medicare Administrative Contractors. The session or memorandum could provide an overview of EFT processes and error-checking and multifactor authentication features that States could consider for their systems, and any insights from CMS's implementation of these features. This information could help inform States that are interested in making similar enhancements to their systems.

Further, CMS could provide States with information regarding matching funds to support improvements to EFT processes or security functions within State claims processing and information retrieval systems.[30] CMS could encourage State Medicaid agencies to share pertinent information from this technical assistance with Medicaid MCOs operating in their States, to the extent allowable by contractual requirements.

After issuing this report, OIG will provide CMS with a nonpublic document containing pertinent survey responses from State Medicaid agencies, which CMS could consider as it prepares this information for States.

Support periodic information sharing among Medicare and Medicaid payors and expert groups to mitigate evolving threats of EFT fraud schemes

To help ensure that security measures keep pace with the evolving nature of EFT fraud schemes, CMS should encourage regular information sharing among Medicare and Medicaid payors, including expert groups as needed (e.g., NIST, HHS Healthcare & Public Health Sector Coordinating Council).

This information-sharing effort could include identifying or establishing a forum to support ongoing information sharing among these entities regarding security expertise, practices to combat EFT fraud, and continuous innovation strategies, as recommended by expert groups. To identify or establish a forum for this information sharing, CMS could:

1) Coordinate with expert groups to identify existing opportunities or venues for information sharing;

2) Identify pertinent groups (e.g., the Administration for Strategic Preparedness and Response[31]) to establish and lead a sharing forum for EFT security information; or

3) Establish a CMS-facilitated working group for information sharing among Medicare and Medicaid payors and amenable expert groups.

These efforts would provide payors with opportunities to learn from expert groups and to discuss new strategies for overcoming barriers or challenges to implementing new processes to mitigate EFT fraud.

AGENCY COMMENTS AND OIG RESPONSE

CMS did not explicitly state its concurrence or nonconcurrence with the first two recommendations and non-concurred with the third recommendation. CMS indicated that the activities described in OIG's first recommendation were already underway and suggested that the recommendation be removed from the report. CMS conveyed that the actions described in the second recommendation were the responsibility of States and were not feasible given limited agency resources; CMS requested that this recommendation also be removed from the report. Finally, CMS non-concurred with the third recommendation, stating that the recommended activities would not be an effective or feasible use of limited resources.

OIG has considered the actions that CMS reported taking and the resource limitations described by CMS in its response. We believe that the recommendations made in this report are reasonable steps that CMS should take to begin expanding upon its existing efforts to detect and prevent EFT fraud. We have adjusted all three recommendations to better clarify how our recommendations offer additional steps CMS should take to protect Federal funds from fraud.

OIG is committed to fighting fraud and will continue to work with CMS to encourage efforts to detect and mitigate evolving EFT fraud schemes in both Medicare and Medicaid. We look forward to CMS's response to the adjusted recommendations in its Final Management Decision.

For the full text of CMS's comments, see Appendix C.

APPENDICES

Appendix A: OIG investigative information on closed cases involving Electronic Funds Transfer fraud schemes (2022–2024)

The table below includes a list of recent prosecutions, restitution amounts, and victims related to Electronic Funds Transfer (EFT) fraud schemes that were investigated by OIG's Office of Investigations.

Case Number	Sentence	Restitution	Medicare and Medicaid Payor Victims
Case 1	48 months	$1,582,510	Texas Medicaid; Washington Medicaid
Case 2	60 months	$4,258,587	Colorado Medicaid; Ohio Medicaid
Case 3	366 days	$626,800	Ohio Medicaid
Case 4	8 months	$57,446	Medicare (Ohio hospital)
Case 5	24 months	$428,525	Medicare (Ohio hospital)
Case 6	37 months	$2,832,755	Medicare (Ohio hospital)
Case 7	24 months	$105,500	Medicare (Ohio hospital)
Case 8	30 months	$703,470	Washington Medicaid
Case 9	18 months	$113,190	Medicare

Source: OIG Office of Investigations case information, 2024.

The table below includes additional details regarding diversion and loss amounts, targeted payors, and law enforcement partners that participated in investigations of EFT fraud schemes along with OIG's Office of Investigations.

Investigation Details	
Total Medicaid and Medicare funds diverted	$26.5 million
Total Medicaid and Medicare funds lost or unrecovered following diversion	$9 million
State Medicaid agencies targeted by scheme	22
Medicare Administrative Contractors targeted by scheme	4
Subjects charged	23
Subjects sentenced	14
Number of law enforcement agencies on investigative team	13: HHS-OIG; Federal Bureau of Investigations; United States Secret Service; IRS-Criminal Investigation; Homeland Security Investigations; Diplomatic Security Service; Minnesota Commerce Fraud Bureau; Federal Deposit Insurance Corporation-OIG; U.S. Department of the Treasury OIG; Wisconsin Division of Criminal Investigation; Missouri Medicaid Fraud Control Unit; Iowa Medicaid Fraud Control Unit; Arkansas Medicaid Fraud Control Unit

Source: OIG Office of Investigations case information, 2024.

Appendix B: Survey responses from Medicare and Medicaid payors

The tables below include results from closed-ended survey questions related to Electronic Funds Transfer (EFT) authorization processes, EFT validation measures, and payor experiences with EFT fraud schemes. The survey was distributed to 76 payors including all 7 Medicare Part A/B Administrative Contractors (MACs) representing 12 jurisdictions, all 56 State and Territorial Medicaid Agencies (States), and 13 Medicaid Managed Care Organizations (MCOs).

Has your agency, entity, or a designee acting on your behalf ever been the target of EFT fraud (actual or attempted)?

	MACs (n=7)	States (n=56)	MCOs (n=13)	Total
Yes	5	33	13	**51**
No	2	23	0	**25**

Source: OIG review of Medicare Administrative Contractor, State Medicaid agency, and Medicaid MCO survey responses, 2024.

Has your agency, entity (including providers enrolled in your network), or a designee acting on your behalf ever experienced financial losses due to EFT fraud?

	MACS (n=5)	States (n=33)	MCOs (n=13)	Total
Yes	2	15	8	**25**
No	3	18	5	**26**

Source: OIG review of Medicare Administrative Contractor, State Medicaid agency, and Medicaid MCO survey responses, 2024.

How does your agency, entity, or a designee acting on your behalf collect information from providers who request to enroll in EFT payments or to make changes to their EFT enrollment information?

	MACs (n=7)	States* (n=56)	MCOs* (n=13)	Total
Provider completes and submits paper EFT authorization or EFT change request form	0	15	2	**17**
Provider enters information in an online provider portal	0	17	5	**22**
Either (provider may complete and submit a paper EFT authorization or EFT change request form, or enter information into an online provider portal)	7	23	5	**35**

*One State Medicaid agency and one Medicaid MCO reported "Other" responses that did not align with the categories above.
Source: OIG review of Medicare Administrative Contractor, State Medicaid agency, and Medicaid MCO survey responses, 2024.

Are there any additional validation processes or security measures that your agency, entity, or a designee acting on your behalf would be interested in implementing to reduce opportunities for EFT fraud?

	MACs (n=7)	States (n=56)	MCOs (n=13)	Total
Yes	3	35	6	**44**
No	4	21	7	**32**

Source: OIG review of Medicare Administrative Contractor, State Medicaid agency, and Medicaid MCO survey responses, 2024.

Has your agency, entity, or a designee acting on your behalf encountered any barriers or challenges related to the implementation of new validation processes or security measures to reduce opportunities for EFT fraud?

	MACs (n=7)	States (n=56)	MCOs (n=13)	Total
Yes	4	16	5	**25**
No	3	40	8	**51**

Source: OIG review of Medicare Administrative Contractor, State Medicaid agency, and Medicaid MCO survey responses, 2024.

DATE: January 16, 2025

TO: Ann Maxwell
Deputy Inspector General
for Evaluation and Inspections

FROM: Chiquita Brooks-LaSure Chiq B LaS
Administrator
Centers for Medicare & Medicaid Services

SUBJECT: Office of Inspector General (OIG) Draft Report: Medicare and Medicaid Payments to Providers Are at Risk of Diversion Through Electronic Funds Transfer Fraud Schemes (OEI-07-23-00180)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft report. CMS is committed to preventing, detecting, and combatting fraud, waste, and abuse in the Medicare and Medicaid programs. To do this, CMS works diligently to prevent fraudulent claims from being paid, and to verify that the right entity is being paid the right amount for covered items and services. This work includes providers, states, and other stakeholders to support proper enrollment, accurate billing practices, and the protection of patients while also minimizing unnecessary burden. In FY 2023, CMS's robust program integrity strategy resulted in estimated Medicare savings of $14.9 billion, and estimated Medicaid and Children's Health Insurance Program federal share savings of $2.3 billion.[1]

CMS directly administers the Medicare fee-for-service (FFS) program and, with support from a network of Medicare Administrative Contractors (MACs), oversees the provider enrollment and screening process for Medicare FFS providers. As noted in the OIG's report, Medicare FFS providers must agree to receive payments via Electronic Funds Transfer (EFT). To do this, providers submit an EFT Authorization Agreement (Form CMS-588) to their respective MAC during their initial enrollment, or when there are any changes to their EFT account information.[2] In addition to submitting the completed Form CMS-588, providers must submit documentation to confirm their account information. Prior to approval, the MACs verify the completeness and accuracy of the information provided.[3] CMS regularly provides the MACs with instructions and guidance on the process that should be used to verify EFT information. Additionally, CMS has directly engaged with individual MACs to provide more targeted technical assistance, and continues to be available to provide these services as needed.

---

[1] CMS, 2023 Report to Congress Medicare & Medicaid Program Integrity, 2024, Accessed at: https://www.cms.gov/files/document/fy2023-medicare-and-medicaid-report-congress.pdf
[2] CMS, Electronic Funds Transfer EFT Authorization Agreement (Form CMS-588), 2023, Accessed at: https://www.cms.gov/medicare/cms-forms/cms-forms/downloads/cms588.pdf
[3] CMS, Medicare Program Integrity Manual Chapter 10 – Medicare Enrollment, 2024, Accessed at: https://www.cms.gov/regulations-and-guidance/guidance/manuals/downloads/pim83c10.pdf

States, as the direct administrators of their Medicaid programs, conduct the screening and enrollment process for providers participating in a state's FFS program and/or that have a network agreement with a managed care plan[4,5]. States are also responsible for developing their own EFT authorization processes, including establishing requirements for collecting and verifying Medicaid providers' EFT information. To support states in their efforts to enroll and revalidate Medicaid providers, CMS allows states to rely on the results of provider screening performed for the Medicare program or other state Medicaid programs.[6] CMS has also published, and updates as needed, the Medicaid Provider Enrollment Compendium, which is a consolidated resource for certain Medicaid provider enrollment regulations and guidance.[7]

The OIG's recommendations and CMS's responses are below.

OIG Recommendation 1

Engage Medicare Administrative Contractors regarding opportunities and barriers to improving security measures for electronic funds transfers, and if appropriate, provide them with technical assistance.

CMS Response

CMS regularly engages with the MACs about opportunities and barriers to improving security measures for EFTs, including providing technical assistance when necessary. Since the activities described in the OIG's recommendation are already underway, and will continue as part of CMS's normal course of business with the MACs, CMS requests that this recommendation be removed.

OIG Recommendation 2

Provide technical assistance to State Medicaid agencies to help address challenges implementing security measures to protect against electronic funds transfer fraud.

CMS Response

Unlike the Medicare FFS program, which is administered directly by CMS, Medicaid is administered by states within federal guidelines. As described above, states are responsible for overseeing the provider screening and enrollment process for their respective Medicaid programs, including establishing their own EFT authorization processes. The time-intensive technical assistance activities described in the OIG's recommendation are not feasible given limited agency resources, and as such CMS requests that this recommendation be removed.

OIG Recommendation 3

Identify or establish a forum to support periodic information sharing among Medicare and Medicaid payors and expert groups regarding security measures to mitigate evolving threats of electronic funds transfer fraud schemes.

---

[4] "Managed care plan" is used here to mean a managed care organization, prepaid inpatient health plan, or prepaid ambulatory health plan, as defined at 42 CFR 438.2.
[5] 42 CFR 438.602(b)
[6] 42 CFR 455.410(c)
[7] CMS, Medicaid Provider Enrollment Compendium (MPEC), 2025, Accessed at: https://www.medicaid.gov/media/123411

CMS Response

CMS non-concurs with this recommendation. While CMS values the importance of cross-payor information-sharing, and sponsors such programs as the Medicaid Integrity Institute and Healthcare Fraud Prevention Partnership, CMS does not believe the activities described in the OIG's recommendation would be an effective use of limited educational resources. As described above, CMS directly administers the Medicare FFS program, while each state administers their own Medicaid program. Given the differences in how the Medicare and Medicaid programs are administered, the recurring and time-intensive activities described in the OIG's recommendation are not feasible or appropriate for CMS to undertake.

ABOUT THE OFFICE OF INSPECTOR GENERAL

Office of Inspector General
https://oig.hhs.gov

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

The Office of Audit Services. OAS provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

The Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

The Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

The Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, the anti-kickback statute, and other OIG enforcement authorities.

ENDNOTES

[1] We also include U.S. Territories and the District of Columbia in the term "State."

[2] U.S. Department of Justice, "10 Charged in Business Email Compromise and Money Laundering Schemes Targeting Medicare, Medicaid, and Other Victims." Accessed on Nov. 18, 2022.

[3] Bloomberg, "Hackers Stole $7.5 million in Grant Money from US Health Department, Jan. 18, 2024." Accessed on July 16, 2024.

[4] 42 CFR § 424.510(e)(1)-(2).

[5] The Medicaid and Chip Payment and Access Commission, "The Medicaid Fee-for-Service Provider Payment Process, July 2018." Accessed on Feb. 9, 2023.

[6] The Health Insurance Portability and Accountability Act of 1996 included administrative simplification provisions requiring the establishment of standards for electronic health information and financial and administrative transactions. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, § 262.

[7] Patient Protection and Affordable Care Act, Pub. L. No. 111–148, § 1104.

[8] 45 CFR § 162.1603.

[9] CAQH CORE, "Operating Rules Mandate: ACA Federal Mandate for Healthcare Operating Rules." Accessed on Mar. 3, 2023.

[10] CAQH CORE, "Payment & Remittance EFT Enrollment Data Rule vPR.1.0 (May 2020)." Accessed on June 5, 2023.

[11] 42 CFR § 424.510(e)(1)-(2).

[12] The CMS-588 Electronic Funds Transfer Authorization Agreement form includes fields to collect a reason for submission, account holder information, financial institution information, and contact person. The form also includes a statement to certify that the account belongs to the provider and to indicate the name and contact information of the authorized or delegated official that is signing the authorization.

[13] CMS, "Medicare Claims Processing Manual, Chapter 1: General Billing Requirements, 30.2.5." Accessed on Jan. 3, 2023.

[14] CMS, "Medicare Program Integrity Manual, Chapter 10: Medicare Enrollment." Accessed on Feb. 22, 2023.

[15] CMS provides State Medicaid agencies with limited access to Medicare enrollment data to facilitate provider screening and enrollment requirements for Medicaid. Center for Medicaid and CHIP services Informational Bulletin, "Medicaid/CHIP Provider Screening and Enrollment." Accessed on Mar. 3, 2023.

[16] State Medicaid agencies with approved State plans may submit Advance Planning Documents (APDs) to request Federal matching funds for the design, development, installation, or enhancement of mechanized claims processing and information retrieval systems. CMS determines whether States' proposed system enhancements are likely to provide more efficient, economical, and effective administration of the State plan, among other requirements and standards, as a condition of funding. Social Security Act § 1903(a)(3)(A)(i); 42 CFR § 433.111(b)(1); 42 CFR § 433.111(b)(2); 42 CFR § 433.112.

[17] OIG, "HHS-OIG Cybersecurity Toolkit: Cybersecurity Considerations for HHS's Rapid Rollout of Information Systems." Accessed on May 1, 2024.

[18] *Reassignment of Medicare Benefits* (OEI-07-08-00180) October 2009.

[19] *Improvements Needed to Ensure Provider Enumeration and Medicare Enrollment Data Are Accurate, Complete, and Consistent* (OEI-07-09-00440) May 2013.

[20] *Reassignment of Medicare Benefits* (OEI-07-08-00180) October 2009.

[21] To expedite this review, this work did not evaluate EFT vulnerabilities in Medicare Parts C and D.

[22] We identified and selected from 128 Medicaid MCO parent companies the largest parent companies by summing the number of enrollees across all respective MCOs that the parent companies operated in any State. The 8 largest Medicaid MCO parent companies each had at least 2 million enrollees and operated 133 Medicaid MCOs total, representing approximately 61 percent of Medicaid MCO market enrollment. We also selected a random sample of 5 mid-size Medicaid MCO parent companies with between 100,000 and 1,999,999 enrollees across all respective Medicaid MCOs that the parent companies operated in any State. Prepaid Inpatient Health Plans and Prepaid Ambulatory Health Plans were not included in the data from which we sampled.

[23] Although we selected Medicaid MCOs on the basis of Medicaid enrollment, some Medicaid MCOs also operate Medicare managed care plans.

[24] Because multifactor authentication comprises the use of more than one distinct authentication factor, and could be achieved by employing varied methods, our survey did not define the term "multifactor authentication."

[25] Medicare Administrative Contractors are subject to requirements established by CMS for EFT processes; therefore, we found that Medicare Administrative Contractors generally reported more consistent practices than did State Medicaid agencies or Medicaid MCOs.

[26] Due to the nature of this survey question, we are unable to determine whether payors employed emails or letters to designated points of contact before or after requested EFT changes were enabled.

[27] In the survey, payors were prompted to describe the validation processes and security measures they employ when providers request to enroll in EFT payments or make changes to their EFT information. Payors were also prompted to describe what makes the validation processes and security measures they employ effective or ineffective in preventing EFT fraud.

[28] CMS's Identity Management (IDM) system is an established, enterprisewide identity management solution. IDM is leveraged by CMS business applications across the agency. End users of all business applications that integrate with this solution can use a single set of user credentials to access any integrated application. CMS, "CMS' Identity Management." Accessed on Mar. 29, 2024.

[29] CMS also implemented error checking features, including mailing address standardization, to improve the accuracy of provider information in CMS systems. CMS, "Identity & Access System Quick Reference Guide." Accessed on Nov. 5, 2024.

[30] Social Security Act § 1903(a)(3)(A)(i); 42 CFR § 433.111(b)(1); 42 CFR § 433.111(b)(2); 42 CFR § 433.112.

[31] The Administration for Strategic Preparedness and Response (ASPR) leads the HHS divisions and works with the public and private partners to provide guidance and support to help enhance cybersecurity for the health care and public health sectors. ASPR, "Healthcare and Public Health Cybersecurity." Accessed on Feb. 19, 2025.

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

OIGatHHS

HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov