2025-10-05-Subject: Urgent — CONFIRMED MALICIOUS CODE in CHFS-issued file (SHA256 e1e63a1f…) — immediate forensic action required

1 message

John Fouts <icreateupwardspirals@gmail.com> Sun, Oct 5, 2025 at 6:17 PM
To: "Perry, Amy S (CHFS DMS DFM)" <AmyS.Perry2@ky.gov>
Cc: "Zimmerer, Zachary M (KYOAG)" <zachary.zimmerer@ky.gov>, KYOAG Appeals <OAGAppeals@ky.gov>, KyOAGOR@ky.gov, "Presley, Stephanie C (KYOAG)" <stephanie.presley@ky.gov>, auditor.mail@ky.gov, govoffice@ky.gov, Office of Governor Beshear <governor.constituentservices@ky.gov>, tbaker@prosecutors.ky.gov, gwhethers@prosecutors.ky.gov, max.comley@ky.gov, mayor@louisvilleky.gov, ic3@fbi.gov, CISA Service Desk <utsprod@servicenowservices.com>, cisaservicedesk@cisa.dhs.gov, ic3@ic3.gov, "Alice Lucas (30th JC)" <alucas@prosecutors.ky.gov>, jprensky@adobe.com, cstoddard@adobe.com, ajassy@amazon.com, jeff@amazon.com, "Wendy Vu (ACI)" <Wendy_Vu@asus.com>, sandy_wei@asus.com, "jackie_hsu@asus.com" <jackie_hsu@asus.com>, jonney_shih@asus.com, "Ryan, Jaime" <Jaime.Ryan@t-mobile.com>, mike.sievert@t-mobile.com, jon.freier@t-mobile.com, "Jones, Shelby L." <shelbyl.jones@uky.edu>, william.thro@uky.edu, amy.spagnuolo@uky.edu, Ellen Kilgore <ellen.kilgore@uky.edu>, pres@uky.edu, Commonwealth Office of Ombudsman <kyombud@ky.gov>, kybar@kybar.org, ky@aclu.org, "Jeff Edwards, P&A Director" <kypandainquiry@gmail.com>, Kevin.McManis@ky.gov, "Smalley, Kevin" <KevinSmalley@kycourts.net>, "Mudd, Sarah G." <sarah.mudd@uky.edu>, charles.griffith@uky.edu
Bcc: fouts.john@gmail.com

Date: 2025-10-05

Subject: Urgent — CONFIRMED MALICIOUS CODE in CHFS-issued file (SHA256 e1e63a1f…) — immediate forensic action required

Amy / CHFS IT team / CHFS CIO:

Forensic reports from independent services (Filescan.io / Falcon Sandbox / VirusTotal) confirm that a file CHFS issued to me contains embedded macros and executable code, outbound routing to third-party hosts (Rackspace) and YARA indicators consistent with credential theft and remote exfiltration (SHA256: **e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9**). I have copies of the triage and analysis reports. This file was delivered to me via the records process CHFS prepared.

This appears to be an **active compromise** used to collect credentials / execute remote commands. I therefore request the following **immediate** actions by CHFS and CHFS IT (please confirm completion by return email within 24 hours):

1. Isolate and preserve the full server and transfer logs for the CHFS system(s) used to generate/transmit the file (MOVEit or any file transfer system used), including timestamps, upload/download logs, user IDs, and all associated metadata and logs for the last 90 days. Preserve backups and snapshots — do NOT delete or overwrite logs.

2. Preserve and export all access logs for the accounts and mailboxes used to send the file and any related outgoing messages.

3. Preserve the original master file on your servers (bit-for-bit copy) and provide a read-only copy or hash to my designated forensic firm or to federal investigators upon request.

4. Explain immediately how the file was generated, the software used to create it, and any contractors/personnel involved. Provide a clear chain-of-custody for the file and show who had access prior to release.

5. Initiate an internal IT incident response (if you have not already) and contact CISA and FBI cyber teams. I am also copying federal oversight agencies and privacy offices for HIPAA/ADA impact.

6. Reissue a clean copy of the requested records **on paper or secure PDF without macros/executables** and provide a secure method for me to download them (SFTP or secure portal) with verification of a checksum prior to opening.

Because this file was delivered as part of your official records production, CHFS bears responsibility to preserve evidence and confirm whether the file was modified intentionally or via compromise. If CHFS cannot or will not preserve logs and cooperate, please notify me in writing immediately and explain why.

I have filed HUD and other civil-rights complaints documenting parallel retaliation and discrimination; those filings are part of the record.

Because this malicious file was transmitted by CHFS through its own records production process, CHFS bears direct responsibility for both the breach and the resulting system compromise.
I therefore demand that CHFS immediately authorize and pay for a **full independent forensic investigation** of my computer and related devices by a **forensic firm of my choosing**, such as Kroll, Mandiant, or CrowdStrike, with the following conditions:

- CHFS shall cover **100% of the cost** of device imaging, malware extraction, and forensic reporting;

- All work shall be done under **chain-of-custody protocol** to ensure admissibility in civil and criminal proceedings;

- The selected forensic vendor shall have **no prior contractual or financial relationship with CHFS** or any Commonwealth IT contractor;

- I shall retain an unredacted copy of all findings;

- CHFS shall cooperate fully by providing access to its MOVEit, file transfer, and email server logs, as well as all metadata associated with the file SHA256 e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9.

Given the proven malicious nature of this file, I also demand that CHFS reimburse me for **all damages already incurred**, including data compromise, loss of equipment use,

and any SSDI garnishments or withheld benefits arising from the same systemic misconduct.

If CHFS has IT or legal counsel who will coordinate with the FBI/CISA/HHS OCR, please identify that point of contact now. I expect a written confirmation of the actions above by no later than 5 p.m. on 2025-10-06 (October 6th, 2025 - no later than 5 p.m. EST).

Additional detailed documentation of financial losses, unreimbursed medical expenses, denied mileage reimbursements, insurance mismanagement, fraudulent refusals to count medical expenses as required by SNAP, wrong amounts used ongoing for medical expenses despite extensive evidence submitted, reimbursement for items insurance was legally bound to cover, shelter expenses marked as $0 that were actually thousands of dollars, fraudulent removal from SNAP (retaliatory), retaliatory intentional miscalculation of SNAP, retaliatory medicaid waiver prohibition of services and goods, and related damages will be provided under separate cover, in addition to other items.

These include—but are not limited to—Medicaid-contracted expenses that were never honored, emergency medical travel costs, replacement equipment required due to the system compromise, and out-of-pocket payments for medically necessary care that were wrongfully denied or delayed.

Each of these losses stems directly from CHFS and affiliated agencies' ongoing violations of ADA, Section 504, 1915(c), VAWA, and HIPAA, and from their refusal to provide reasonable accommodations and lawful reimbursements.
Upon delivery of the itemized summary, I will require full reimbursement, restitution, and correction of all account records, including SSDI-related garnishments, within an urgent, yet reasonable, timeframe.
--

Sincerely,

/s/ John R. Fouts

John R. Fouts, MBA
Son of a Vietnam-War-Era Veteran
Founder, *Upward Spirals Association* (508(c)(1)(A) Spiritual Faith-Based Organization – Protected under RFRA)
Federal SSA SSDI Recipient – Protected under ADA, VAWA, Section 504, and 1915(c)
Mainstream Voucher Holder – HUD/IHCDA/CASI Program

Email: **icreateupwardspirals@gmail.com**
Alternate: **torchoftruth@zohomail.com**
Phone (Text Only – ADA Accommodation): **502.956.0052**

Voice calls & voicemails will be ignored
Fax (HIPAA Compliant): **604.641.2805**

Evidence archive (prior to block on saving):
https://archive.org/details/@jfouts1979

---

30 attachments

2025-10-05-Amy-Perry-CHFS-Xcitium-Cloud-Malware-High-Classification-VirusTotal - IP address - 74.125.201.95.pdf
119K

2025-10-05-Amy-Perry-CHFS-VirusTotal - IP address - 92.38.145.145.pdf
102K

2025-10-05-Amy-Perry-CHFS-VirusTotal - File - e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9.pdf
221K

2025-10-05-Amy-Perry-CHFS-VirusTotal - IP address - 74.125.201.95.pdf
118K

2025-10-05-Amy-Perry-CHFS-Further-Information-VirusTotal - IP address - 92.38.145.145.pdf
485K

2025-Amy-Perry-CHFS-10-05-Classified-As-Malware-By-Abusix-VirusTotal - IP address - 173.194.206.102.pdf
104K

2025-10-04-Amy-Perry-CHFS-Additional-Malware-Found-Report-UK-Ireland-Google-e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9 _ Triage.pdf
102K

2025-10-04-Amy-Perry-CHFS-Suspicious-Files-Filescan.io - Analysis Report for e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9 - Threat_indicators.pdf
254K

!2025-10-04-Amy-Perry-CHFS-FileScan-Report-of-File-Received-Via-MoveIt-e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9-68e1c76cd4a0085473c064b1 (1).pdf
150K

2025-10-04-AMY-PERRY-CHFS-Free Automated Malware Analysis Service - powered by Falcon Sandbox - Viewing on.pdf
704K

e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9-68e1c76cd4a0085473c064b1.pdf
150K

2025-10-04-Amy-Perry-CHFS-Exact-Match-Malicious-Page5-Filescan.io - Advanced Report Search Results.pdf
112K

2025-10-04-Amy-Perry-CHFS-Exact-Match-Malicious-Page6-Filescan.io - Advanced Report Search Results.pdf
65K

2025-10-04-Amy-Perry-CHFS-Exact-Match-Malicious-Page4-Filescan.io - Advanced Report Search Results.pdf
119K

2025-10-04-Amy-Perry-CHFS-Exact-Match-Malicious-Page3-Filescan.io - Advanced Report Search Results.pdf
113K

2025-10-04-Amy-Perry-CHFS-Exact-Match-Malicious-Page2-Filescan.io - Advanced Report Search Results.pdf
114K

2025-10-04-Amy-Perry-CHFS-Further-Lookup-2-Filescan.io - Advanced Report Search Results-Shows-Many-As-Malicious-Part-2.pdf
140K

2025-10-04-Amy-Perry-CHFS-Further-Lookup-2-Filescan.io - Advanced Report Search Result-Shows-Suspicious-Part-3.pdf
88K

2025-10-04-Amy-Perry-CHFS-Exact-Match-Malicious-Page1-Filescan.io - Advanced Report Search Results.pdf
113K

2025-10-04-Amy-Perry-CHFS-Further-Lookup-2-Filescan.io - Advanced Report Search Results-Shows-Many-As-Malicious.pdf
148K

2025-10-04-Amy-Perry-CHFS-Further-Lookup-1-Filescan.io - Advanced Report Search Results.pdf
89K

2025-10-04-Amy-Perry-CHFS-Suspicious-Yara-Rules-Filescan.io - Analysis Report for e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9 - Yara.pdf
324K

2025-10-04-Amy-Perry-CHFS-Records-IP-Lookup-Through-Whois-Icann-Org-Part-3-ICANN Lookup-Rackspace-San-Antonio-and-Unknown-Registrant-Address-Bulgaria.pdf
91K

2025-10-04-Amy-Perry-CHFS-Records-IP-Lookup-Through-Whois-Icann-Org-Part-1-ICANN Lookup.pdf
124K

2025-10-04-Amy-Perry-CHFS-Records-IP-Lookup-Through-Whois-Icann-Org-Part-2-ICANN Lookup.pdf
122K

2025-10-04-Amy-Perry-CHFS-Further-Analysis-Why-Embedded-Macros-Filescan.io - Analysis Report for e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9 - Threat_indicators.pdf
322K

2025-10-04-Amy-Perry-CHFS-Forensic-Analysis-Recommended-Filescan.io - Analysis Report for e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9 - Details.pdf
381K

2025-10-04-Amy-Perry-CHFS-Further-Analysis-Why-Embedded-Macros-Filescan.io - Analysis Report for e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9 - Threat_indicators-2.pdf
315K

2025-10-04-Further-Analysis-Amy-Perry-File-CHFS-Filescan.io - Analysis Report for e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9 - Details.pdf
401K

2025-10-04-Amy-Perry-CHFS-Records-Results-Suspicious-Filescan.io - Analysis Report for e1e63a1f1c25c6410837bcf4c0f718fa40333936d140f666d21f1f7eb55326a9 - Overview.pdf
372K