Financial Sector Cyber Information Group

CIG Circular 66 – FASTCash ATM Cash Out Campaign

Date: 10/2/18

TRAFFIC LIGHT PROTOCOL (TLP): WHITE – SUBJECT TO STANDARD COPYRIGHT RULES, TLP:WHITE INFORMATION MAY BE DISTRIBUTED WITHOUT RESTRICTION.

Treasury is providing this Circular to inform the financial services sector about newly identified HIDDEN COBRA activity involving a cyber campaign targeting retail payment system infrastructure. This Circular includes an overview of the activity, details of the fraud scheme, technical analysis, and detection and mitigation recommendations. We are also releasing this information with DHS and FBI today in TA18-275A on https://www.us-cert.gov/hiddencobra. Activity associated with this campaign should be given the highest priority for enhanced mitigation and reported to the FBI or DHS's National Cybersecurity and Communications Integration Center.

OVERVIEW

Treasury has identified a sophisticated cyber-enabled ATM cash out campaign we are calling FASTCash. FASTCash has been active since late 2016 targeting banks in Africa and Asia to remotely compromise payment switch application servers within banks to facilitate fraudulent transactions, primarily involving ATMs, to steal cash equivalent to tens of millions of dollars. FBI has attributed malware used in this campaign to the North Korean government. We expect FASTCash to continue targeting retail payment systems vulnerable to remote exploitation.

FASTCash targets retail payment system infrastructure within banks to enable fraudulent ATM cash outs across national borders. FASTCash uses interactive malware to deploy and configure applications on compromised switch application servers probably to intercept financial request messages and reply with fraudulent but legitimate-looking affirmative response messages.

- While we do not know the initial infection vector, all of the affected servers identified were running unsupported IBM AIX operating systems beyond their end of service support date; however, we have no evidence FASTCash exploited the AIX operating system in these incidents.
- According to a trusted partner, the amount of cash stolen in known incidents is estimated to be tens of millions of dollars.
- In one known incident from early 2018, FASTCash conspirators concurrently withdrew cash from ATMs in 23 countries by conducting over 10,000 transactions in under five hours. FASTCash conspirators withdrew cash from ATMs in over 30 countries during a separate incident in late 2017. We have no insight into how the conspirators transmitted the cash from the withdrawal sites back to those orchestrating the campaign.

FASTCash uses knowledge of standardized financial transaction interchange messaging in addition to general purpose malicious cyber techniques to exploit target systems. FASTCash deployed ISO 8583 libraries on targeted switch application servers, most likely to assist with the interpretation of financial request messages and to appropriately construct fraudulent financial response messages. ISO 8583 is the international standard for financial transaction card originated interchange messaging.

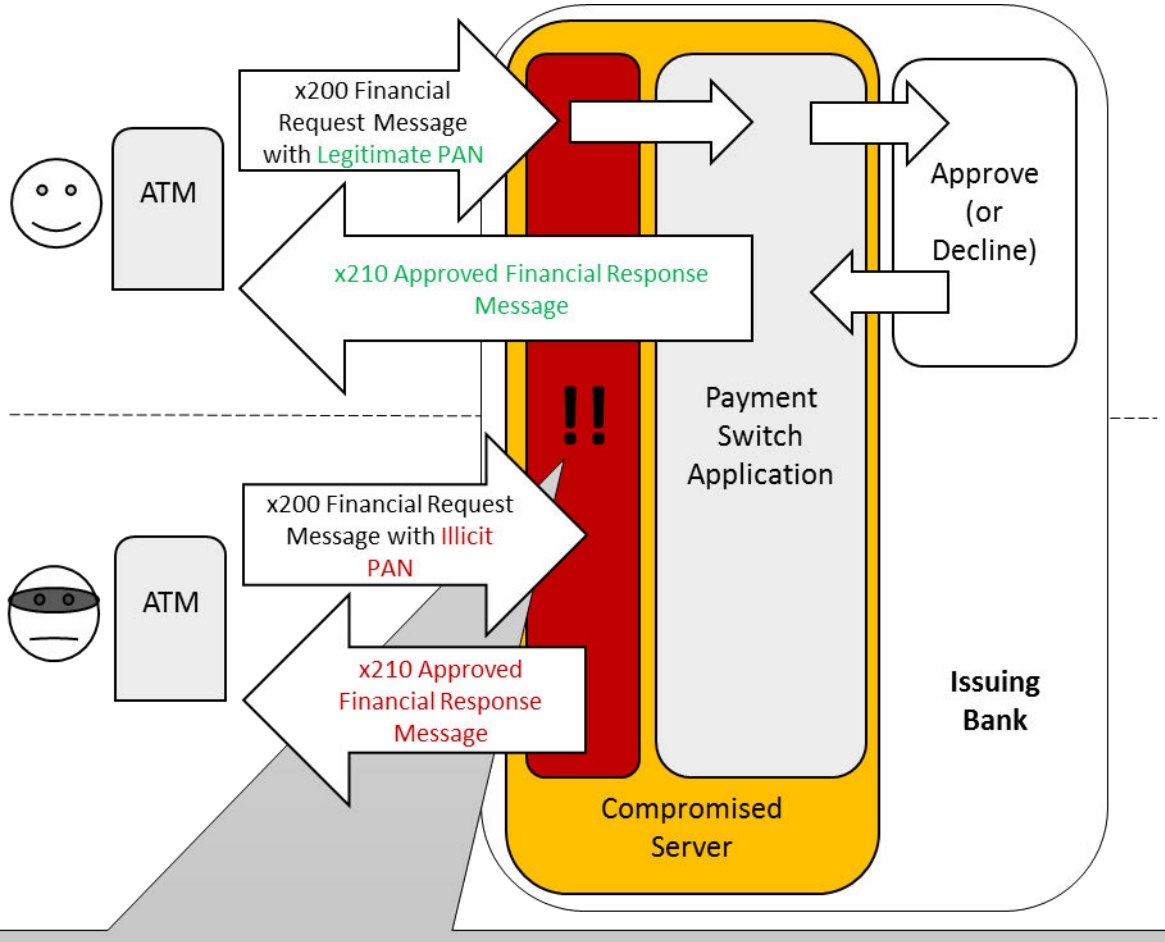
- FASTCash deployed malware to enable remote interactions, including through the command line, with the switch application server. Log files captured FASTCash making typos and other mistakes, and actively correcting errors when configuring the targeted server to enable the scheme.
- FBI has attributed FASTCash malware to the North Korean government. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https://www.us-cert.gov/hiddencobra.
- Scripts found on affected systems indicate FASTCash inspected inbound financial request messages for specific primary account numbers (PANs) and generated fraudulent financial response messages only for the request messages matching expected PANs. Accounts with the PANs used to initiate the transactions mostly had minimal account activity or zero balances.

Where were the FASTCash incidents? Are they related to any recent activity?

Treasury has confirmed three FASTCash incidents affecting unnamed institutions outside the United States. **At this time, Treasury has NOT confirmed any FASTCash cyber incidents affecting institutions inside the United States.** We used forensic artifacts from two of these three incidents to prepare this report. Artifacts from the third incident were not available to us for analysis.

As of publication, we do not have enough information to definitively link the widely reported August 2018 ATM cash out incident in India to FASTCash. The technical aspects of this fraud scheme appears to have been directed at the switch application server, according to many press reports, which is a technique that has been unique to FASTCash. The widespread withdrawal activity and the scale of associated monetary loss reported in the press also align with those of known FASTCash incidents.

ANATOMY OF THE SCHEME



- An application running on the compromised switch application server probably inspects inbound Financial Request Messages at the transport layer for particular account numbers using a CheckPan() function.
- If the Request Message does NOT contain one of the pre-identified illicit PANs, the payment switch application processes the message and routes it appropriately to the issuer.
- If the Request Message contains a pre-identified illicit PAN, the application probably generates a fraudulent Response Message using the GenerateResponseTransaction1() or GenerateResponseTransaction2() function to respond to the acquirer with a fraudulent Response Message and drops the Request before the payment switch application processes the message, leaving the issuer with no knowledge of the transaction.
- The application appears to have the capability to intercept and block declined Response Messages from the switch to the ATM, presumably as a check in case the switch receives the fraudulent request and passes in on to the issuer.

TECHNICAL ANALYSIS

FASTCash used malicious Windows executables, command-line utility applications, and other files to perform transactions and interact with financial systems, including the switch application server.

We do not know the initial infection vector FASTCash uses but suspect spear phishing against the targeted banks' employees. After the initial compromise, FASTCash most likely used Windows based malware to monitor and explore the bank's network to identify the payment switch application server. FASTCash used different, but mostly functionally equivalent, malware in each known incident.

All of the payment switch application servers known to be targeted by FASTCash were the same proprietary UNIX platform running an unsupported IBM AIX operating system already past its end of life. We have no evidence FASTCash exploited this operating system. More likely, FASTCash illicitly accessed the server using legitimate credentials obtained during their monitoring and exploration of the bank's network, suggesting FASTCash may have used compromised systems within the bank's network to exploit the access the payment switch application server.

We are also not aware of any UNIX based malware used by FASTCash. FASTCash, however, appears to have deployed scripts using command line utility applications on the payment switch application server to illicitly enable fraudulent behavior by the system in response to what would otherwise be normal payment switch application server activity, as depicted in the diagram above.

FASTCash probably used AIX executable files designed to inject code and libraries into a currently running process. One AIX executable provides export functions, which allows an application to manipulate transactions on financial systems using the ISO 8583 standard.

FASTCash executed .so commands in each incident using the following pattern:

```
/tmp/.ICE-unix/e <PID> /tmp/.ICE-unix/<filename>.so <argument>
```

The Process ID, filename, and argument varied between targeted institutions; however, the malicious executable named "e" appeared in the /tmp/.ICE-unix directory in all cases. This directory typically contains X-windows session information.

One malicious script contained a similar but slightly different command:

```
./sun 30671054 /tmp/.ICE-unix/engine.so  [with argument "0" or "1"]
```

FASTCash also injects or ejects the following libraries:

- `m.so [with argument "0" or "1" for inject or eject]`
- `m1.so [with argument "0" or "1" for inject or eject]`
- `m2.so [with argument "0" or "1" for inject or eject]`
- `m3.so [with argument "0" for inject or eject]`

DHS NCCIC conducted analysis on four Windows based malware samples, two command line utility applications, and three applications designed to provide export functions and methods to allow the application to interact with financial systems all recovered from two separate FASTCash incidents and produced a Malware Analysis Report (MAR). Below is an overview of the artifacts but please refer to

MAR-10201537 on https://www.us-cert.gov/hiddencobra for the full report and associated indicators of compromise.

Windows Executables

Name:	Unknown
MD5:	5cfa1c2cb430bec721063e3e2d144feb
Description:	Themida packed 32-bit Windows executable designed to unpack itself and run a service proxy module in memory. The proxy module accepts command line parameters and is designed to modify the Windows Firewall on the compromised system to allow incoming connections and function as a backdoor. The malware listens on a specified port for incoming traffic containing instructions to perform any of the following functions: retrieve system information; execute commands; execute and terminate processes; search for files; read, write, and delete files; download and upload files; and, compress and decompress files.

Name:	Unknown
MD5:	4f67f3e4a7509af1b2b1c6180a03b3e4
Description:	Themida packed 64-bit Windows executable with the same functionality as 5cfa1c2cb430bec721063e3e2d144feb and is signed with a valid X509 certificate issues to "A-Z Hire Ltd" with serial number: EC:AF:E7:23:70:36:14:E0:A4:FB:5C:2A:8F:7D:A0:18[1]

Name:	Unknown
MD5:	d0a8e0b685c2ea775a74389973fc92ca
Description:	32-bit Windows executable designed to execute as a service named "helpsvcs". The malware binds and listens on port 443 for incoming connections, providing remote command and control capabilities through this connection. The malware uses the RC4 encryption algorithm to encrypt and decrypt a portion of its communications and has the ability to exfiltrate data, install and run secondary payloads, and provided proxy services on the compromised system. This malware can perform the following functions based on specified commands from a remote operator: retrieve system information; execute commands; execute and terminate processes; search for files; read, write, and delete files; download and upload files; compress and decompress files; and, change the listening port for Remove Desktop via registry modification. d0a8e0b685c2ea775a74389973fc92ca also contained the following hardcoded IP address: 75[.]99[.]63[.]27 using port 443[2]

[1] *CIG Circular 65 – APT-Connected RAT Associated with Financial Sector Intrusion Activity Related to Fraudulent Use of SWIFT* identified this same code signing certificate used in some of the implants discussed in the Circular.

[2] We are providing this IP address for information purposes only.

Name:	Unknown
MD5:	8efaabb7b1700686efedadb7949eba49
Description:	Malicious 64-bit Windows Dynamic Link Library designed to runs as a Windows services under “svchost.exe” and load an RC4 decrypted payload into memory.

AIX Command Line Utility Applications

Name:	Injection_API_executable_e
MD5:	b3efec620885e6cf5b60f72e66d908a9
Description:	AIX executable intended for a proprietary UNIX operating system developed by IBM. This application injects a library into a currently running process.

Name:	inject_api
MD5:	58bb2236e5aee39760d3e4fc6ee94a79
Description:	AIX executable, intended for a proprietary UNIX operating system developed by IBM and is designed to update a proprietary data structure on a UNIX system known as "PVPA."

AIX ISO 8583 Specific Applications

Name:	Lost_File1_so_file
MD5:	d790997dd950bb39229dc5bd3c2047ff
Description:	AIX executable, intended for a proprietary UNIX operating system developed by IBM. This file is a library application designed to provide export functions. These functions allow an application to perform transactions on financial systems using the ISO 8583 standard.

Name:	2.so
MD5:	b66be2f7c046205b01453951c161e6cc
Description:	AIX executable, intended for a proprietary UNIX operating system developed by IBM. The application provides several exported methods permitting the interaction with financial systems that utilize the ISO 8583 standard.

Name:	Lost_File.so
MD5:	46b318bbb72ee68c9d9183d78e79fb5a
Description:	COFF executable, a format for executable, object code, and shared libraries used on UNIX systems. The executable provides several exported methods that enable interactions with financial systems utilizing the ISO 8583 standard.

In addition to the analysis of the artifacts above, the below IP addresses may be associated with the FASTCash Campaign.[3] Mail servers in the compromised network made reverse proxy connections to these IPs but we do not have specific date and time stamps or other information to associate them with malicious activity:

167[.]114[.]33[.]205

180[.]235[.]133[.]108

219[.]255[.]99[.]9

DETECTION AND MITIGATION RECOMMENDATIONS

1. Contact law enforcement immediately regarding any identified activity related to FASTCash. Please see contact information for FBI and DHS NCCIC at the end of this report.
2. Incorporate the indicators of compromise identified in DHS's Malware Analysis Report MAR-10201537 on https://www.us-cert.gov/hiddencobra into intrusion detection systems and security alert systems to enable active blocking or reporting of suspected malicious activity.
3. Review bash history logs of all users with root privileges. Commands entered by users can be found here and would indicate the execution of malicious scripts on the switch application server. All commands should be logged and monitored. Log files associated with known incidents exhibited the commonalities identified below.

Recommendations for Institutions with Retail Payment Systems

Require Chip and PIN Cryptogram Validation

- Implement Chip and PIN requirements for debit cards.
- Validate card-generated authorization request cryptograms.
- Use issuer-generated authorization response cryptograms for response messages.
- Require card-generated authorization response cryptogram validation to verify legitimate response messages.

Isolate Payment System Infrastructure

- Require two factor authentication for any user to access the switch application server.
- Confirm perimeter security controls prevent Internet hosts from accessing the private network infrastructure servicing your payment switch application server.
- Confirm perimeter security controls prevent all hosts outside of authorized endpoints from accessing your system, especially if your payment switch application server must be Internet accessible.

Logically Segregate your Operating Environment

- Use firewalls to divide your operating environment into enclaves.
- Use access control lists to permit/deny specific traffic from flowing between those enclaves.

[3] We are providing these IP addresses for information purposes only.

- Give special considerations to segregating enclaves holding sensitive information (e.g., card management systems) from enclaves requiring Internet connectivity (e.g., email).

Encrypt Data in Transit

- Secure all links to payment system engines with a certificate based mechanism, such as MTLS, for all traffic external or internal to your organization.
- Limit the number of certificates that can be used on the production server and restrict access to those certificates.

Monitor for Anomalous Behavior as Part of Layered Security

- Configure the switch application server to log transactions and routinely audit transaction and system logs.
- Develop a baseline of expected software, users, and logons and monitor switch application servers for unusual software installations, updates, account changes, or other activities outside of expected behavior.
- Develop a baseline of expected transaction participants, amounts, frequency, and timing. Monitor and flag anomalous transactions for suspected fraudulent activity.

Recommendations for Organizations with ATM or POS Devices

Validate Issuer Responses to Financial Request messages

- Implement Chip and PIN requirements for debit cards.
- Require and verify message authentication codes on issuer financial request response messages.
- Perform authorization response cryptogram validation for CHIP and PIN transactions.

Recommendations for All Organizations

Treasury reminds users and administrators to use the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and require regular password changes.
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, and configure it to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.

- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the Internet before executing.
- Maintain situational awareness of the latest threats.
- Implement appropriate access control lists.

Additional information on malware incident prevention and handling can be found in NIST's Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops:

https://www.nist.gov/publications/guide-malware-incident-prevention-and-handling-desktops-and-laptops

Why Best Practices Matter

The National Security Agency recently published its *Top Ten Cybersecurity Mitigation Strategies* (https://www.iad.gov/iad/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm). Aligned with the NIST Cybersecurity Framework, the *Strategies* offer a risk-based approach to mitigating exploitation techniques used by Advance Persistent Threat (APT) actors. While all of the strategies are important, Treasury has highlighted each mitigation strategy in the *Strategies* below that may have mitigated known FASTCash incidents in part or whole based on our understanding of FASTCasg tactics, techniques, and procedures. The non-highlighted items probably would have assisted in detection and recovery.

The *Strategies* counter a broad range of exploitation techniques used by APT actors. NSA's mitigations set priorities for enterprise organizations to minimize mission impact. The mitigations also build upon the NIST Cybersecurity Framework functions to manage cybersecurity risk and promote a defense-in-depth security posture. The mitigation strategies are ranked by effectiveness against known APT tactics. Additional strategies and best practices will be required to mitigate the occurrence of new tactics.

1. Update and Upgrade Software Immediately
Apply all available software updates, automate the process to the extent possible, and use an update service provided directly from the vendor. Automation is necessary because threat actors study patches and create exploits, often soon after a patch is released. These "N-day" exploits can be as damaging as a zero-day. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to assure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender's patch cycle.
2. Defend Privileges and Accounts
Assign privileges based on risk exposure and as required to maintain operations. Use a Privileged Access Management (PAM) solution to automate credential management and fine-grained access control. Another way to manage privilege is through tiered administrative access in which each higher tier provides additional access, but is limited to fewer personnel. Create procedures to securely reset credentials (e.g., passwords, tokens, tickets). Privileged accounts and services must be controlled because threat actors continue to target administrator credentials to access high-value assets, and to move laterally through the network.

3. Enforce Signed Software Execution Policies

Use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. Maintain a list of trusted certificates to prevent and detect the use and injection of illegitimate executables. Execution policies, when used in conjunction with a secure boot capability, can assure system integrity. Application Whitelisting should be used with signed software execution policies to provide greater control. Allowing unsigned software enables threat actors to gain a foothold and establish persistence through embedded malicious code.

4. Exercise a System Recovery Plan

Create, review, and exercise a system recovery plan to ensure the restoration of data as part of a comprehensive disaster recovery strategy. The plan must protect critical data, configurations, and logs to ensure continuity of operations due to unexpected events. For additional protection, backups should be encrypted, stored offsite, offline when possible, and support complete recovery and reconstitution of systems and devices. Perform periodic testing and evaluate the backup plan. Update the plan as necessary to accommodate the ever-changing network environment. A recovery plan is a necessary mitigation for natural disasters as well as malicious threats including ransomware.

5. Actively Manage Systems and Configurations

Take inventory of network devices and software. Remove unwanted, unneeded or unexpected hardware and software from the network. Starting from a known baseline reduces the attack surface and establishes control of the operational environment. Thereafter, actively manage devices, applications, operating systems, and security configurations. Active enterprise management ensures that systems can adapt to dynamic threat environments while scaling and streamlining administrative operations.

6. Continuously Hunt for Network Intrusions

Take proactive steps to detect, contain, and remove any malicious presence within the network. Enterprise organizations should assume that a compromise has taken place and use dedicated teams to continuously seek out, contain, and remove threat actors within the network. Passive detection mechanisms, such as logs, Security Information and Event Management (SIEM) products, Endpoint Detection and Response (EDR) solutions, and other data analytic capabilities are invaluable tools to find malicious or anomalous behaviors. Active pursuits should also include hunt operations and penetration testing using well documented incident response procedures to address any discovered breaches in security. Establishing proactive steps will transition the organization beyond basic detection methods, enabling real-time threat detection and remediation using a continuous monitoring and mitigation strategy.

7. Leverage Modern Hardware Security Features

Use hardware security features like Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Platform Module (TPM), and hardware virtualization. Schedule older devices for a hardware refresh. Modern hardware features increase the integrity of the boot process, provide system attestation, and support features for high-risk application containment. Using a modern operating system on outdated hardware results in a reduced ability to protect the system, critical data, and user credentials from threat actors.

8. Segregate Networks Using Application-Aware Defenses

Segregate critical networks and services. Deploy application-aware network defenses to block improperly formed traffic and restrict content, according to policy and legal authorizations. Traditional intrusion detection based on known-bad signatures is quickly decreasing in effectiveness due to encryption and obfuscation techniques. Threat actors hide malicious actions and remove data over common protocols, making the need for sophisticated, application-aware defensive mechanisms critical for modern network defenses.

9. Integrate Threat Reputation Services
Leverage multi-sourced threat reputation services for files, DNS, URLs, IPs, and email addresses. Reputation services assist in the detection and prevention of malicious events and allow for rapid global responses to threats, a reductioan of exposure from known threats, and provide access to a much larger threat analysis and tipping capability than an organization can provide on its own. Emerging threats, whether targeted or global campaigns, occur faster than most organizations can handle, resulting in poor coverage of new threats. Multi-source reputation and information sharing services can provide a more timely and effective security posture against dynamic threat actors.
10. Transition to Multi-Factor Authentication
Prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets. Physical token-based authentication systems should be used to supplement knowledge-based factors such as passwords and PINs. Organizations should migrate away from single factor authentication, such as password-based systems, which are subject to poor user choices and susceptible to credential theft, forgery, and reuse across multiple systems.

REPORTING FASTCash ACTIVITY

To report an intrusion and request resources for incident response or technical assistance, contact DHS NCCIC (NCCICCustomerService@hq.dhs.gov or 888-282-0870), FBI through a local field office (https://www.fbi.gov/contact-us/field-offices) or FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937).

The Financial Sector Cyber Information Group (CIG) was established within the Department of the Treasury, Office of Critical Infrastructure Protection and Compliance Policy in 2013. The CIG monitors and analyzes all-source information on cyber threats and vulnerabilities to the financial sector; provides timely, actionable cyber threat information to the sector; and solicits feedback and information requirements from the sector. Please take a moment to let us know:

Does this Circular provide information that is not available to you elsewhere?
Is the information provided actionable?
Is the level of context appropriate?

Please direct any comments or questions to CIG@Treasury.gov.

Eligible stakeholders can download CIG Circulars and other relevant government information from the DHS Homeland Security Information Network (HSIN) Financial Services Portal. For information on membership, download the quick guide from: http://go.usa.gov/3YH45