**ETOC: Dos and Don’ts**

*This document explains some of the ETOC work principles: what we are not to do, how we should handle ourselves, what processes we should follow and how to ensure information security while providing proper customer service.*

ETOC employees can access a lot of **sensitive information** and perform some highly **sensitive changes**. We are also being constantly contacted by people from outside of WU organization, so we must ensure that we are not providing any sensitive information or do any sensitive changes without proper approvals and following proper guidelines.

Having **access to Production environment**, we should also make sure we are using it only for authorized testing, and we are properly processing testing data afterwards.

We are also **conducting remote sessions** to agent computers, so we should make sure we are not doing anything what is not necessary and may affect their computer setup.

Resetting passwords

**Do not reset any passwords, PC Signatures, unlock accounts!**

Although we have access to reset passwords, PC signatures, etc, **ETOC is only authorized to do the reset for ETOC use**: when you need to reset password for your user/operator or PC Signature for terminal which you created.

We should **not** reset passwords even if:

* Regional Operations Manager (ROM) is asking to do it for agent or for himself/herself
* You are on a remote session with agent, and agent is not able to login
* Internal WU employee who you know (or don't know) is asking for help
* Agent Operator is having login issues, and Call Center/Agent Support) was not able to help (we investigate the root cause, but do not reset the password).
* You want to test using agent's terminal, but it has a PC Signature captured.

This applies to WUPOS, Trackpayments, and other passwords and security features, **except**:

* Login to SafeNet portal for Agent/ROM. With approval from Regional operations we can unlock/resync tokens for agent Operators, who are managing agent's tokens. We do not unlock/resync tokens for WUPOS, ARC+, etc, only for SafeNet portal login. We also do not unlock/resync tokens for Call Center operators.
* Voyager ADMIN user password reset. We do provide queries and assist agent to login to Voyager, but we do not do it for WAD/Trackpayments, SFG users.

Operators, terminals, certificates

**Do not create operators, users, terminals and provide certificates to customers, agents, other teams or employees!**

ETOC is only authorized to create operators, terminals, users and download certificates for our own use (testing, issue replication). There are no exceptions for this rule, doesn't matter who is asking for it.

**This applies to all systems accessible to ETOC.**

Security features

**Do not enable, disable or edit any security features, Send, Pay, Modify, Cancel options and Compliance setup without SERVICENOW self-service request from ROM.**

Security features, features allowing agent to record, pay or modify transaction and compliance setup are the most sensitive features ETOC can edit, so even if there is an email or a call from ROM, **we must insist for them to raise a formal request via SERVICENOW**. With the request there is a clear accountability of who requested and who completed the change.

If ETOC is doing some testing and needs to apply such changes, they can only be applied on the engineering accounts or Terminals, created by ETOC. **No active agent accounts should be ever updated** without an SERVICENOW request.

Sensitive information

**Do not share any sensitive information!**

With our accesses, we can see a lot of sensitive information, but we should be careful when sharing it. **Sensitive information includes:**

* MTCNs
* Account, Operator, Terminal IDs
* Sender/Receiver details, compliance information
* Log fragments containing such data
* Screenshots of our internal systems and tools
* Compliance rules

When investigating the issue, we may need to provide any or all of above to the teams troubleshooting the issue, but we must ensure not to provide it to:

* Agents and ROMs
* Any external contacts not directly involved into troubleshooting
* Any internal employees not directly involved into troubleshooting

*For example:*

* We can share logs, screenshots from tools with the 3rd Level team investigating the issue, but when contacting Agent or ROM, who reported that issue, we should remove any such information.
* If agent has provided MTCNs, Accounts, Terminals to ETOC, we can use them in further communication. But if they did not provide this information and we found it in our systems, we should not be sharing it with them.
* ETOC should be responding agent with root cause and how to solve it, not with MTCN information, our system logs, etc.

Documentation

**Do not share any internal Technical Documentation without approval from InfoSec and Legal departments!**

Only approved documentation can be shared with agents (such as approved Voyager guides). Any new guides and material must first get all required approvals and only then can be shared with the Agents.

Any technical documentation available to ETOC should not be shared with agent (such as Documents of Understanding, technical specifications, diagrams, escalation documents) without prior **approval from Infosec and Legal departments**.

You may share some instructional screenshots and short step by step instructions with the agents in your emails, but first make sure that screenshots do not have any sensitive information.

For example, it is ok to share step by step instruction how to clear Java cache, as long as the screenshots do not contain any details about your computer or other unnecessary information. However, if you have a document, outlining all Java related troubleshooting steps and information, it must be approved before

Testing

**Do cancel all MTCNs completed via testing!**

Make sure that any MTCN completed via testing is canceled. If MTCN was paid, it needs to be unpaid and canceled.

**Do not record, pay or edit any real customer MTCNs!**

If you require to test recording, paying or editing MTCN, make sure you are using test MTCN and test data. Do not use real names, real customer ID information or exiting MyWU card.

**Do not send D2B, Quick Pay, Make Payment, Quick Collect transactions!**

***They cannot be refunded!***

If this is required for testing purposes:

* Get ETOC manager approval
* Get test credentials and test receiving account

Remote sessions

**Do leave functioning and clean system after your remote session!**

If you have been installing Voyager: make sure that all updates and patches are installed and agent is able to import files.

If you have created several Voyager DBs for testing: make sure you leave only the one (or ones) used by agent, delete the test DBs.

If you have installed several SQL server instances: make sure you remove all unused ones.

If you have installed WUPOS certificate several times: make sure to leave just one.

If you changed some computer configuration, and it did not help to solve the issue: change it back.

Cleanup after investigation

**Delete all unnecessary data, certificates, databases after investigation!**

A lot of data we use for investigation is very sensitive and protected by privacy laws. If you have downloaded agent Settlement and Activity files, logs, etc, to your personal computer, make sure to delete them once you are finished with investigation.

If you have created terminals, accounts or operators for testing, delete them, once you are done.

If you have created ARC+ profile for your testing, delete it afterwards.