­­<Company> Systems, Inc.

Intelligent Automation

Security, Risk and Compliance Management

Confidential

Table of Contents

[Introduction 3](#_Toc527768740)

[Scope of Intelligent Automation Security 3](#_Toc527768741)

[Bot deployment scenarios 4](#_Toc527768742)

[Unattended Bot Deployment 4](#_Toc527768743)

[Attended Bot deployment 5](#_Toc527768744)

[Hybrid Automation 6](#_Toc527768745)

[Bot Deployment Infrastructure 6](#_Toc527768746)

[On Employee Workstation 6](#_Toc527768747)

[On Dedicated ‘Bot Station’ 7](#_Toc527768748)

[RPA Security Requirements 7](#_Toc527768749)

[Internal Audit Perspective 7](#_Toc527768750)

[Align RPA Security to Enterprise IT Security 8](#_Toc527768751)

[Security During Design & Development 9](#_Toc527768752)

[Assignment of Bot IDs 9](#_Toc527768753)

[Credential Management 10](#_Toc527768754)

[End to End Data Protection 10](#_Toc527768755)

[Encryption Keys and the Credential Vault 10](#_Toc527768756)

[Data at Rest Encryption 10](#_Toc527768757)

[Data in Motion 11](#_Toc527768758)

[Data in Use 11](#_Toc527768759)

[Vulnerability Testing 11](#_Toc527768760)

[Penetration Testing 12](#_Toc527768761)

[Regulatory Compliance 12](#_Toc527768762)

[Customer specific compliance requirements 12](#_Toc527768763)

[Standard IT compliance requirements 12](#_Toc527768764)

[Review of RPA Security Controls 13](#_Toc527768765)

[Appendix A: <Company> Bot ID generation process 14](#_Toc527768766)

# Introduction

This document describes approach, processes and recommended practices for ensuring security and compliance for Intelligent Automation deployments at <Company>. To ensure appropriate Enterprise Risk Management (ERM) and IT risk management and governance controls, it is important to put in place security, compliance and risk management policies and processes to pre-empt the probability of security violations during design, development and operation of Bots at <Company>. These policies need to take into account and align with existing IT compliance and other relevant ERM requirements already in place at <Company>

# Scope of Intelligent Automation Security

The objective of this Bot Security and Compliance guideline is to complement existing IT governance, risk and compliance policies in place at <Company>. It provides best practice guidance and reference for development and operations using Intelligent Automation Bots while integrating such Bot-specific practices into existing <Company> IT compliance policies. Once deployed, RPA becomes an integral

part of the enterprise IT infrastructure, and its security should also be acceptably integrated and compliant with the same exacting requirements as expected of Enterprise IT Security.

Therefore these guidelines cover key risks and security concerns introduced by RPA such as:

* Authorization & Authentication
* Credential Management
* Secure Bot Development Lifecycle
* Data Security & Encryption
* Data Retention Policies
* Penetration/Vulnerability
* Anti-Malware protection
* Infrastructure Security

As is likely obvious, RPA security implies that all existing mandatory IT security practices need to be followed to the highest level of diligence. Areas that are mandatory for IT security are not treated in-depth in this document. This does not imply that any basic information security standards should be neglected.

Emerging Technologies

As Intelligent Automation includes several rapidly emerging technologies including RPA (Robotic Process Automation), AI and ML (Artificial Intelligent & Machine Learning), OCR (Optical Character Learning), ChatBots etc., these guidelines are planned taking into consideration the secured integration and operation of such new technologies as required in future. This will enable <Company>’s Intelligent Automation COE and <Company>’s business units and business process owners to evaluate, develop and operate Bots in future while continuing to stay compliant with IT compliance requirements.

# Bot deployment scenarios

Bots are scripts that work on the UI or ‘front-end’ of software applications. They mimic a human operator’s actions, thereby allowing humans to assign routine, rule-based and high-volume tasks to Bots. This enables gaining greater productivity and frees up time for human operators by automating mundane tasks and putting in valuable human efforts into more value adding work.

Bots can be designed and deployed to operate in any of following configurations:

1. Unattended mode
2. Attended mode
3. Hybrid mode

Each mode of Bot deployment and operations has its own set of unique security implications.

Automation in above listed modes gives companies versatility and flexibility in deploying automated processes depending on:

* Degree to which process can be automated in view of available technology capabilities
* Desirability of automation depending on how desired To Be process needs to mix Bots and human actions
* Integration of need for human supervision
* Workload planning and requirements
* Budgetary constraints and planning
* Any other particular aspects of operational processes.

The various modes of Bot deployment enable flexibility, feasibility and speed of automation deployment without disrupting or changing work processes. This enables organizations to begin their Intelligent Automation journey early and start reaping benefits from the value brought by existing Intelligent Automation technologies as not all end-to-end processes may be completely automatable as Unattended Automation in a first phase deployment.

### Unattended Bot Deployment

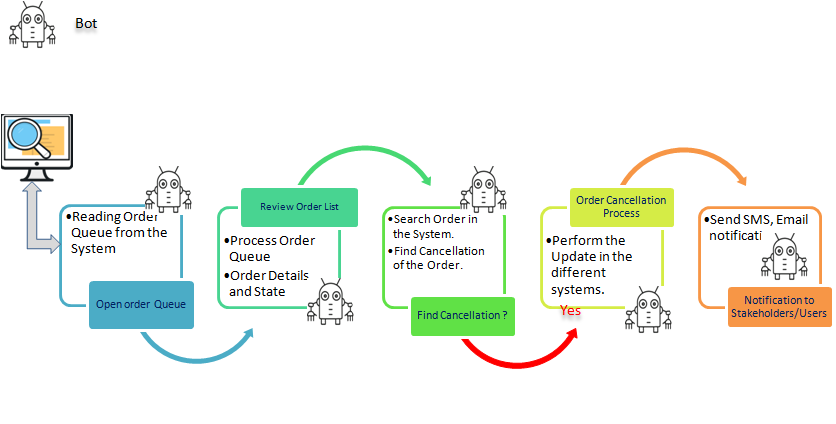
In Unattended mode, Bots automatically perform process steps with NO human intervention.

All actions are automatically triggered and acted upon by Automation Bots themselves and work is accomplished continuously in a batch-mode model. This automation allows availability for carrying out actions on a “24 x 7 x 365” schedule if required. Unattended automation is deployable in a wide range of IT topology and configurations such as on physical or virtual workstations, VMs, VDI, servers as per client expectations.

The only human intervention required is by an Automation Administrator who can view, analyze, deploy, schedule, audit, monitoring, modify versions and generally administer the automation using a central management console.

Unattended automation is a desirable state to attain the fullest value from RPA deployment. However, it may not always be achievable unless all process steps and exceptions are clearly defined. It may also be difficult to achieve unattended automation in cases where exceptions or errors are likely to occur in a process that require human operators to review cases before the bot can proceed further. The Start and End points of Unattended Bots may be designed so as to ensure that no human interaction is required during any step of the Bot’s operation. If human input is required, then such human interaction can be done after Bot has completed its output where this is feasible and suited to the needs of the business process.

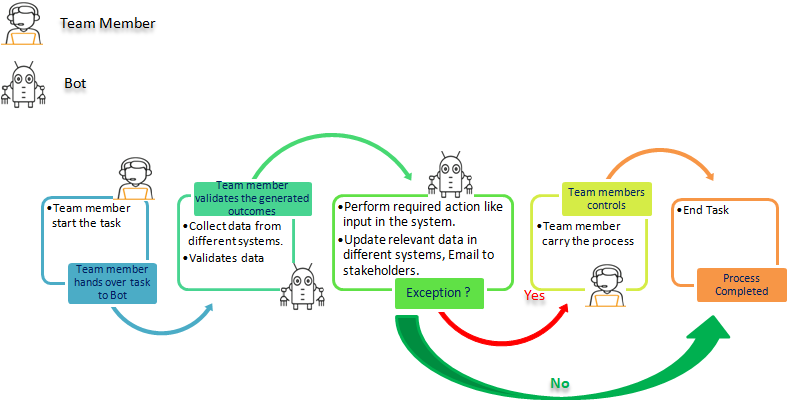
Image below depicts a fully-automated process using a Bot to perform all actions.



### Attended Bot deployment

In Attended mode, Bots cannot perform all steps required to complete the end to end process by themselves and MUST have specified human intervention to complete execution. Such Bots require actions or inputs from a human operator to either initiate, proceed or terminate based on Specific inputs provided by a human operator. While a process can be broken down into two or more sub-processes to enable unattended bot operations to the extent possible, this may not be desirable from an overall process from a business perspective. In such cases, Attended automation provides a practical alternative to enable human operators to benefit from Automation while continuing to focus their skills and competencies on solving cases where the Bot may not have the required skills.

Image below depicts a Attended Automation process using both a human operator and a Bot to perform actions to complete end to end process.



### Hybrid Automation

In a future state it is envisioned that human operators and Bots can send tasks back and forth to each other to complete multiple processes. For the purpose of this document and given the maturity of Intelligent Automation technology available in market today, this state is some time into the future. We shall consider such Hybrid automation scenarios as part of Attended automation for the purpose of our Intelligent Automation approach. However, in planning for the overall infrastructure for enabling Bots it is important to note that the approaches we take today should allow us to adapt to such high volume and frequent scenarios of Bot and human interactions.

# Bot Deployment Infrastructure

In above deployment modes, automation may be deployed in one or a combination of following topologies:

### On Employee Workstation

Bots may be hosted within physical or virtual workstation of a particular employee or group of employees i.e., particular department/process or in virtual environments where Bot performs its actions in an instance allocated to the Bot. Which means features of Bot is available to limited team members who are engaged in a certain workflow in a specific workstation or department. From a provisioning, security and tracking perspective this means that both user (human operator) and bot have access to the same machine. Provisioning of ID for bot needs to be managed appropriately to ensure that actions performed by Bot and human operator can be separately tracked. There will also be Bots which are initiated by human operator’s actions, as against Bots which will be automatically triggered and ‘seek’ human interactions. Such human operator actions and Bot actions need to be clearly tracked.

Attended automations increase potential for enabling human workers to control Bots. Such attended automation can be enabled by allowing for sufficient separation of human and bot actions.

There are instances where unattended automation is also deployed on human operator’s workstation. This may be done by providing appropriate credentials to Bots to log-in to workstations by using Auto-Login, Run Bots and then Log-off from workstation when human operator is not using the workstation. Unattended bots may also run on human work-stations as a background task when human operator is using the work-station. This can be achieved securely using separated Bot and Human user IDs.

### On Dedicated ‘Bot Station’

Where possible Bots should be deployed on physical or virtual stations that is accessed only by a Bot or multiple Bots with appropriate credentials. Some such Bots may require intermediate human intervention to complete their processing. If so human operator will interact with Bot as per specified workflow via a separate interface, workflow or other action initiated by the Bot on the user’s machine.

Unattended automations should be typically deployed in VMs where feasible to ensure full-benefits of automation.

# RPA Security Requirements

## Internal Audit Perspective

RPA offers the potential to deliver sizable improvements in productivity and cost while increasing compliance and risk coverage. Unlike humans, who may skip a process step, or may make other errors in processing transactions, a bot can perform the task in a standard manner, free of bias or any variation, thus delivering upto 100% accuracy levels. But RPA can also introduce risks if appropriate controls are not in place and monitored. For instance, because RPA action is consistent, any error becomes a systemic and widespread issue across that business process and data set. Or, if there is a business process change but the robot has not been modified to reflect that change, it may fail to perform or introduce inaccuracy. If someone gains unauthorized access to a robot, it could be altered or used to conduct unauthorized transactions.

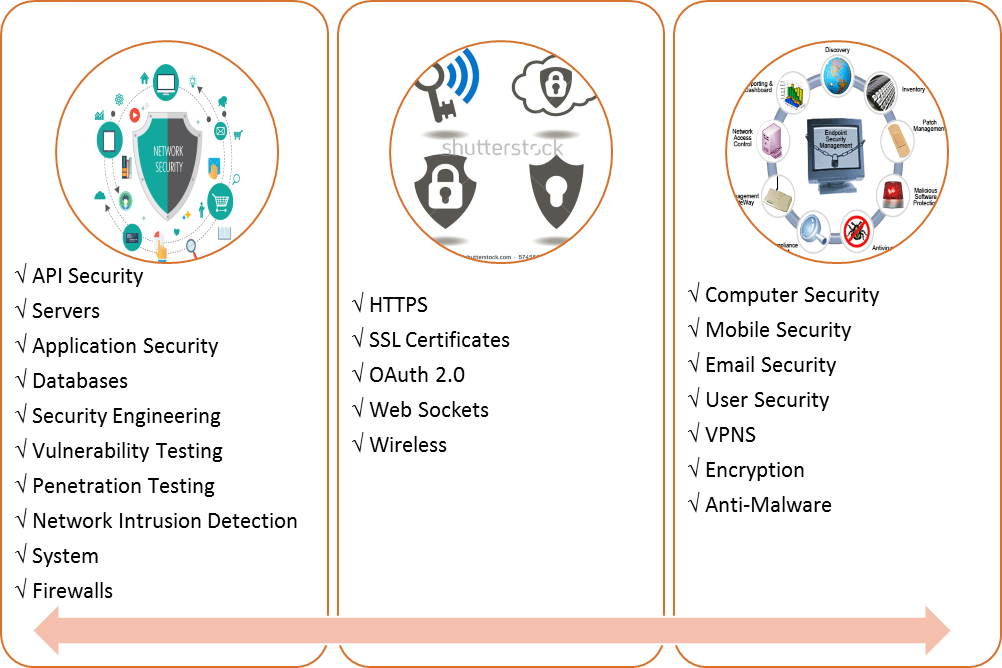
Internal Audit teams need to understand how their organization is planning to use Intelligent Automation (RPA & other technologies) and how this may impact its risk profile. Establishing governance of RPA and relevant controls up front should help effectively mitigate risks and speed up RPA deployment by thinking broadly about exposure across multiple categories of risk as indicated in table below. By embedding governance, risk management, and controls into the enterprise’s planning and deployment of RPA, organizations can catch issues before they arise. Getting it right from the start is far more effective and cost efficient from an Internal Audit perspective than creating compliance processes, policies and controls later.

|  |  |
| --- | --- |
| Risk Category | Key Questions |
| Executive | Who owns the overall RPA initiative for the organization?  Who is developing a company-wide governance framework for RPA? |
| Technical | How will control of the robot’s access to systems and data be handled?  How will robots be tested to make sure they function as intended? |
| Change Management | Has management considered the impact the RPA program will have on human resources?  How are communications being managed? |
| Operational | What controls exist to monitor performance?  How will the business stay compliant with relevant regulatory requirements? |
| Functional | Who designs controls?  Are there scalability limitations in RPA and core systems? |

Internal audit’s early involvement in an RPA initiative ensures a balanced discussion, risk assessment and agreement on internal controls, risk management and compliance processes. As with other IT and organizational compliance requirements, Internal Audit guidelines for risk management, mitigation and overall enterprise risk management need to be adhered to by the Intelligent Automation processes for design, development and operational use of Bots.

## Align RPA Security to Enterprise IT Security

As noted earlier, all the RPA infrastructure and deployments must allow enforcement of all elements of IT security as depicted below:



**Network Security**

**Internet, Cloud, Wireless Security**

**End Point Security**

As <Company>’s IT security & compliance adheres to ISO 27001 requirements all RPA implementations need to be compliant with the relevant requirements and controls for design, development and deployment of any software elements integrated with IT infrastructure.

From an RPA security perspective the following areas are identified as critical:

1. **Use Unique Credentials for Bots**
   * Assign a unique identity to each Bot
   * Use multifactor authentication and rotate passwords for each Bot account
   * Do not allow hardcoding of credentials within Bot scripts
   * Make use of a credential store mandatory to avoid inadvertent user credential misuse
2. **Beware of Breaks in Segregation of Duties**

* Separate developers and bot operators
* Enable privileged session management when Bot deployments lead to privileged accounts
* Provide strict auditing and monitoring for fraud management, when segregation of duties is unavoidable

1. **Ensure the RPA Tool Provides a Full Audit Trail** 
   * Ensure that RPA product provides a proper audit log
   * Ensure audit log is customizable to address <Company> specific needs
2. **Ensure RPA Tool provides Essential IT Security and Compliance Features** 
   * Verify that the RPA tool supports <Company> IT standards for data and password encryption, other security compliance features
   * Test the RPA product using standard security and vulnerability testing tools
   * Address compliance risks
3. **Secure the Complete RPA Life Cycle, Not Just the Operation**
   * Review and test each Bot (RPA Scripts)
   * Provide for change control for Bots (RPA Scripts)

## Security During Design & Development

Security is an important consideration from Design stage. Practices followed during design and development stage should be compliant with <Company> enterprise IT security policies for data access, secure access to customer information, userids and passwords. It is desirable that the RPA tool supports secure Bot development practices such as masking userids and passwords in design stage if required.

## Assignment of Bot IDs

Assign a unique identity to each Bot. Ensure Bot IDs and privileges are created using a defined process early in the design & development lifecycle. Bots should have dedicated identification credentials whenever possible.

**Nomenclature:** Bot ID naming should distinguish between human and bot identities wherever possible. There is not one single right way to implement this in practice. One example could be assigning B-123 as an identity for the bot operated by an employee with the identity E-123.

**Attended & Unattended Operation:** Bot ID should be able to support operation and auditability for both attended and unattended operations.

[**Appendix A**](#_Appendix_A:_Ryder) provides existing process for creating a new Bot ID at <Company>.

## Credential Management

Secure credential management enables removal of embedded and locally stored credentials from Bots, and allows these highly-sensitive passwords and SSH keys to be centrally secured, managed and audited.

Identity and access management options available for enterprise deployments, include:

* LDAP, include Active Directory using LDAP, Active Directory using Kerberos
* SAML 2.0 based single sign-on
* Integration with 3rd-party privileged access/credential management solutions (e.g., CyberArk, One Identity,and Thycotic)

**Credential Store:** It is highly recommended that all Bots use a credential store for managing all IDs and access credentials, preferably one that is integrated as part of the RPA product.

**Role Based Access Control (RBAC):**

Bot Authentication is only the first step of access control enforcement for secured Bot operation. Ensuring fine-grained Role Based Access Control (RBAC) by adhering to the core principles of least privileges and separation of duties is critical to ensuring compliance in complex enterprise scale Bot deployments. The RPA product should enable support for such RBAC functionality.

## End to End Data Protection

The RPA platform should provide safeguards that not only protect data at rest and in transit, but also while it is in use on individual systems during design, development and operation.

### Encryption Keys and the Credential Vault

As discussed earlier a Credential Vault is used to store all system managed credentials and critical system configuration data. It can also be used to store any other sensitive data (e.g., name-value pairs) used in an organization’s automations. As a result, Bot developers can avoid the insecure practice of hard-coding credentials and other sensitive data/arguments directly within their automations.

### Data at Rest Encryption

The RPA Product or Credential Store should provide secure storage for sensitive configuration parameters and details pertaining to the integral version control and email services. Typically encryption requirement is for using AES 256 bit encryption for data at rest.

### Data in Motion

The RPA product should require use of Transport Layer Security (TLS) 1.2 to assure data security and

integrity during transport between components.

Ideally Bot credentials should also be encrypted prior to being submitted over a TLSs ecured

connection. This extra layer of encryption not only protects against network stack issues (such as Heartbleed), but also prevents exposure of the credentials for implementations where the outerlayer TLS connection is terminated at a front-end load balancer.

**OAuth:** OAuth is an open-standard authorization protocol or framework that describes how unrelated servers and services can safely allow authenticated access to their assets without actually sharing the initial, related, single logon credential. In authentication parlance, this is known as secure, third-party, user-agent, delegated authorization.

### Data in Use

Data security when Bots are in production begins with distributed credential protection.

This can be enforced by requiring no local credential storage on environment that are running Bots.

Credentials and other data dynamically retrieved from the Credential Vault for use within automations should be retained solely in encrypted format in volatile memory – and be wiped out as soon as the associated bot is finished executing.

Other options to consider in the RPA product to prevent unauthorized access to confidential information or tampering with bots during runtime include:

* Stealth mode – where no program windows are displayed on the local screen and logged in users have the option to disable image capture during Bot design and Bot operation, thereby preventing sensitive information displayed on-screen from being stored in bots
* Input lock – the ability to disable the mouse and keyboard for the machine where an automation is running
* Time limit – the ability to set a time limit after which an automation will be terminated if it has not finished executing
* Central control – the ability to centrally control (i.e., pause, resume, stop) the operation of remotely running automations from within the a single Management Console

## Vulnerability Testing

As discussed earlier, the RPA Platform and Bots should be tested for Vulnerability using standard tools. Each new release and upgrade of the RPA platform and bot upgrades should be required to undergo the testing requirement. <Company> IT Security standard tools or vendor should be used for this purpose.

Few tools that can be used for this include Owaps ZAP, BlackDuck, Veracode, Nessus.

## Penetration Testing

The RPA Platform and Bots should be Penetration Tested to determine if exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application. Penetration tests find exploitable flaws and measure the severity of each. A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system.

Few tools that can be used for this include BurpSuite, SQL MAP, Nmap, Wireshark.

## Regulatory Compliance

<Company> systems ERM (Enterprise Risk Management) and IT compliance requires compliance with SOX, HIPAA, GDPR (for UK business) and other regulatory compliance regulations. The RPA platform should enable compliance for such regulations.

[Full list of <Company> regulatory compliance requirements required]

## Customer specific compliance requirements

RPA product should support field level customization for additional security and compliance requirements as per customer specific obligations.

[Full list of customer specific compliance requirements required]

# Standard IT compliance requirements

In addition to the focus on RPA specific IT security requirements, it is important to follow IT compliance discipline to all aspects of the Bot design, development, operations and updation processes. Some of these are highlighted below:

* **Permission Matrices:**  There should be strict adherence to permission matrices with respect to permissions for all Bots in design, development and production. e.g. Read-only, Administrator, Creator, Modify etc.
* **Monitoring Communications:** There should be monitoring tools in place to identify in/out communication with respect to any devices, IP. Few tools that are typically used include Nagios, Telerik Fiddler, NetworkMiner etc.
* **Scanning Attachments:** Any external/internal attachment must be scanned before download/use.
* **Restricting & Monitoring Attachments:** Email attachment should be restricted with the respect to size or has to be scanned through before going out of the network.
* **Backup Policy**: Apply standard <Company> IT backup policy unless there are more stringent business & process specific compliance requirement. In which case the latter shall be applied. It is recommended to have incremental backup everyday and full backup every month.
* Best practices must be followed for:
  + **Event/Audit log** have to be monitored
  + **Password policy, access rights/controls**
  + **Network command** restricted
  + **Check-Lists:** It is recommended to have appropriate checklists for: Data access, Device access, Email, Registration, User creation, Application / Utility /Hardware installation, etc.
* **Approval for New & Updates to Software & Access:** Require approval from authority for new software installation and access network /machine. For installing/add/edit/delete, Bot, application, new hardware, etc.

# Review of RPA Security Controls

Compliance and controls for RPA and related technologies have to be periodically reviewed and appropriately adjusted for the various elements of RPA and IT security.

Security Audit: It is recommended to have security audit every 6 months and have discussion/review with stakeholders for improvement and fill gaps if any.

# Appendix A: <Company> Bot ID generation process

Following is the process for requesting accounts for Bots at <Company>:

RAR to create appropriate AD ID:

* Create New User Request
* Select **User Type**:  “Contractor”  (this is temporary until the RAR can accommodate RPA account requests)
* First Name, Last Name:  (suggest naming convention related to appropriate application or process for the business process or business workflow)
* [David F added additional items here in blue]
  + For **email** use [firstname\_lastname@<Company>.com](mailto:firstname_lastname@ryder.com)
  + For **job title** use RPA Robot
  + **location code** use the location code of the team it is “working for”
  + In the **comments** section enter:  Add to “GG\_RPA”
  + NEXT
  + **Domain** should be HQ
  + Click LAN and EMAIL, plus any specific access the bot will eventually need.
  + NEXT
  + Make the **expected date** “today”
  + The approver should be someone in the team the bot is working for
  + SUBMIT

What happens next:

* RAR will generate a CON # and ID Management Team will replace the prefix “CON” with “RPA”.
* ID Management will reply to the requestor with account details once the account is created.
* The current RAR will generate an email 30 days prior to account expiration.  The manager/requestor of the RPA will need to request an extension of access for another 90 days by approving the request or rejecting it.  If no extension request, the RPA account will expire upon 90 day timeframe from when it was created.
* GG\_RPA will be used for additional controls and restrictions

Above process with effect from: 19 Sept 2018

[We should have SLA for Bot ID creation]

[If ID problems then how is this addressed]

[Contact ID, person in case of any ID issues]