Secure Credit Card or Direct Debit Transactions-1701

Introduction

Use **extreme caution** when handling sensitive customer information

- With identity theft so prevalent, we make every effort to ensure a customer's personal information is not compromised

Resolution Steps

Please adhere to the following guidelines:

1. Ensure you are **speaking** with the **cardholder** before processing Credit card or Direct Debit Transactions

2. **Never** use **paper and pen** or a **Notepad** program to record Social Security, Credit Card, or Direct Debit banking information, and then enter it into BOLT / ICOMS

    - **Always** input this information **directly** to the correct field

3. **Never enter** the customer's Social Security Numbers, Credit Card numbers, of Direct Debit account numbers **into your account notes**

    - This is **not** a secure place for this information

4. **Never send** a customer's Social Security Number, Credit Card number, of Direct Debit account number **with a messaging** technology (email, instant messaging, text, etc.)

    - This is **not** a secure place for this information

5. **Always** make certain that you entered the correct Credit Card or Direct Debit information by reading the account numbers, and expiration dates back to the

customer

6. The customer's unencrypted Social Security number, credit card number, or direct debit banking information is **not to be shared** with anyone **inside** or **outside** the organization