Anatomy of an *Interac*® chip debit card transaction

Chip technology securing *Interac* Debit, ABMs and *Interac* Flash™

Interac debit cards equipped with chip technology will be standard by the end of this year. Ever wonder what goes on when you put your card in a Point-of-Sale (POS) terminal or an ABM, and what it means to you? Let's look at how it all works at a POS terminal.

The Players:

Interac Debit Card

Chip – it's like a mini computer on your card

Point-of-Sale (POS) Terminal

Chip enabled terminal – built in security to conduct chip transactions

Financial Institution

Interac Inter-Member Network – setting rules and standards and facilitating the transaction

Chip technology gives the card the ability to store and process data securely and makes it extremely difficult to copy and reproduce. This processing power is used with cryptography to secure the transaction "conversation" that occurs between your *Interac* debit card, the POS terminal, and your financial institution via the *Interac* Inter-Member Network.

Sending the data by cryptogram ensures that the information cannot be interpreted by anyone else. Cryptography is the science of keeping confidential messages secure using mathematical algorithms with the purpose of encrypting data.

It only takes seconds to process an *Interac* Debit transaction. During this time, a complete 12-question "conversation" happens in a 4-step security process.

The Four Steps Of Transaction Security:

1. Payment Selection

As soon as you insert your *Interac* chip debit card into the POS terminal, the secure transaction conversation begins. The terminal first determines that you want to pay with *Interac* Debit and then prompts you to enter your PIN.

2. Validation

The payment terminal asks your card for the data required to proceed with the transaction and authenticates you as the cardholder. This process includes security checks like making sure that your card's effective and expiration dates are valid. The terminal also performs a test to ensure that your card has not been tampered with.

3. Risk Control

Your financial institution then joins the conversation. Once the terminal and your card have made the decision to proceed, data is sent online to your financial institution in a format only they can interpret, which they validate through their own security analysis.

4. Completing Your Transaction

Once your financial institution decides it is safe to proceed and there are funds in your account to pay for your purchase, the data is sent back by cryptogram for your card to authenticate. Your card then makes the decision to approve and complete the transaction, bringing the conversation to a conclusion.

Added Security:

Under *Interac* rules, *Interac* chip debit cards cannot allow for fall-back. This means that if a criminal copied the magnetic stripe on your card and captured your PIN, then tried to use that fake mag stripe card at a chip POS terminal or ABM, the conversation process would identify this and decline the transaction.