The Fraud Department Call

1 You Receive a Call

You receive a call or text from your bank or credit card company's fraud department. The caller ID on your phone matches the company they claim to be from.

2 The Scammer Provides Info

The rep provides your name, address, sometimes even the last 4 digits of your account number.

3 "Rep" Claims Unusual Activity

The rep verifies that certain purchases were not yours. They ask you to verify your identity by providing your account PIN and/or provide your full account number.

4 They Send you a Code

The rep may even send a verification code to your cell phone and ask you to repeat it back to them to "cancel those charges."

IMPORTANT: If someone calls or texts claiming to be from your bank or credit card company, hang up and call the number on the back of your card.

No fraud department should ever ask you to confirm your PIN

You can **NOT** trust caller ID. It's called '**spoofing**' and scammers can impersonate any organization.

The fact that the caller has **SOME** of your info already **does not mean** that they are who they say they are.

Your **account number, PIN** and **verification code** are **key factors** scammers require. **Never share them**!

Combatting cybercrime through collaboration

KnowledgeFlow.org

Durham Regional Police

Town of Ajax By the Lake

Victim Services Durham Region

KnowledgeFlow Cybersafety Foundation