# Data Breach Alert:

## Inside the Capital One Data Breach

## What Happened

### 106 million

PII data of roughly 106 million Capital One customers/applicants were breached — which was detected 4 months after it occured.

### 14-Year-Span

Data from customers & small businesses that applied for Capital One credit cards between 2005-early 2019 were impacted.

### 140,000

Roughly 140K SSNs and 80K bank account numbers were exposed

### $150-$500 Million

The initial cost of the data breach is estimated to be between $150-$500 million

## What You Need to Know

- ➢ No fraud is expected on current existing bank card portfolios based on info stolen
- ➢ New account fraud, digital wallet fraud (Zelle) and takeover fraud are the primary issues that could occur.
- ➢ Fraud could occur at other financial institutions with new accounts opened with stolen data.
- ➢ Potential fraudulent account openings using SSNs and other credentials stolen from the breach could cause issues to evolve for years.

## What To Do About It

- ❑ Educate cardholders about the incident, how to track incidents and freezing their credit.
- ❑ Inform cardholders about common fraud scams that could occur like fraudulent accounts.
- ❑ Offer extra fraud/credit monitoring to proactively protect your customers.
- ❑ Ask cardholders if they have applied for a Capital One card during the breach and incorporate the information into the banks KYC process
- ❑ Monitor potential fraud In real-time to get ahead of incidents before they spread.
- ❑ Track the fallout of the breach to identify potential Incidents from compromised data.

Rippleshot

Stopping Fraud at the Speed of Data