GM sectec 50 YEARS

WWW.GMSECTEC.COM

OFFERING SERVICES

CLIENTS IN OVER
50 COUNTRIES

GLOBAL PRESENCE

OVER
50 THOUSAND
CLIENTS ENROLLED

GROWING

WITH MORE THAN
3 THOUSAND
SECURITY PROFESSIONALS

STRATEGIC ALLIANCE

WITH PR SCIENCE,
TECHNOLOGY AND RESEARCH
TRUST & POLYTECHNIC
UNIVERSITY OF PR

- SAN JUAN
- PANAMA CITY
- FT. LAUDERDALE
- MEXICO CITY
- SAO PAULO
- SANTIAGO
- BOGOTA
- MADRID
- MELBOURNE

EFFICIENCY

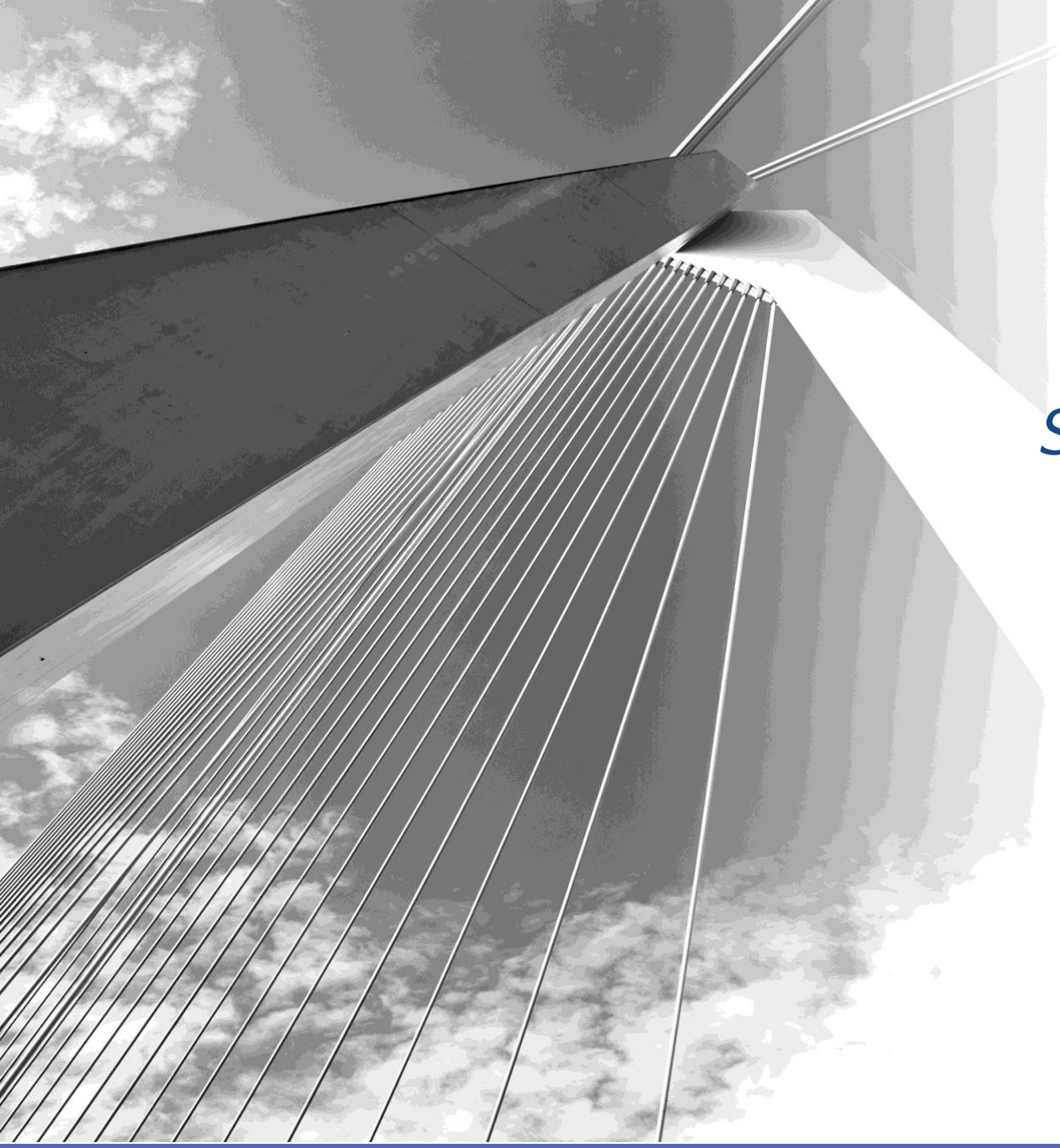
CONTROL

CHOICE

PREFERRED PARTNER

VISA | GM sectec

PCI APPROVED SCANNING VENDOR
PCI QUALIFIED SECURITY ASSESSOR
PCI P2PE - QUALIFIED SECURITY ASSESSOR
PCI 3DS ASSESSOR
PCI PA-DSS QUALIFIED SECURITY ASSESSOR
PCI CARD PRODUCTION SECURITY ASSESSOR
PCI QUALIFIED PIN ASSESSOR
PCI PCI FORENSIC INVESTIGATOR
UL LISTED
FIRST



In eComm We Trust

Securing Payments and Disrupting the Cybercrime Pandemic

The Next Generation of Commerce: Are you ready?

acdet
Asociación Comercio al Detal de Puerto Rico

March 04, 2021

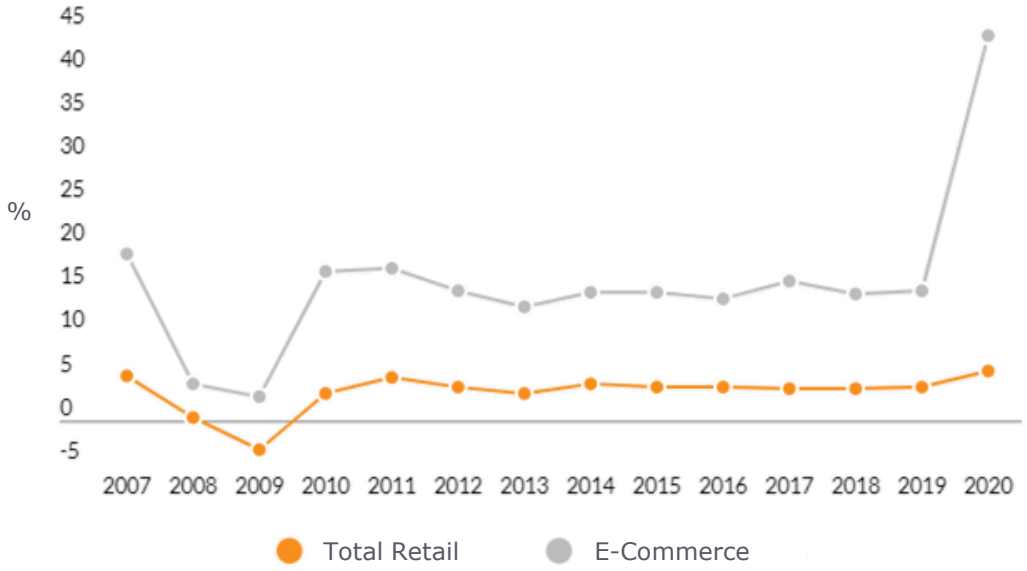
GM sectec

Contents

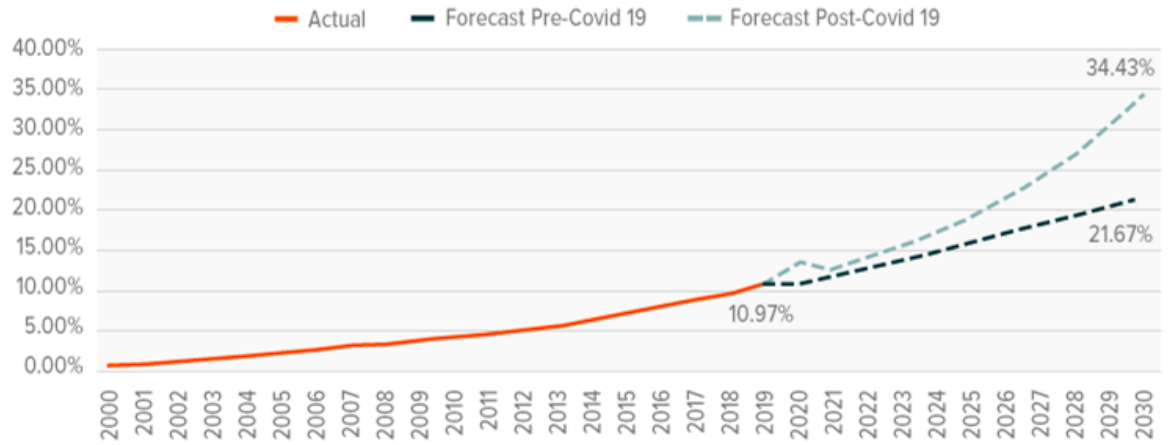
E-Commerce Before and After COVID-19

The global pandemic re-charted the foreseeable path for retail online commerce

Year-on-Year Growth
Total US Retail vs. E-Commerce Sales



*US E-Commerce Penetration**
Pre-COVID 19 vs. Post-COVID 19



Actual E-Commerce as % of Total Retail Sales (as released per US Census Bureau) **for 2020**:

Q1 11.8%
Q2 16.1%
Q3 14.2%
Q4 14.0%

After a sharp initial spike, online ***retail sales have outperformed expectations***

Why?

Sources and graphs: Digital Commerce 360; Global X ETFs; US Census Bureau – Monthly Retail Trade, 4Q 2020 E-Commerce Report

* Forecasted figures based on confirmed 1H 2020 confirmed sales

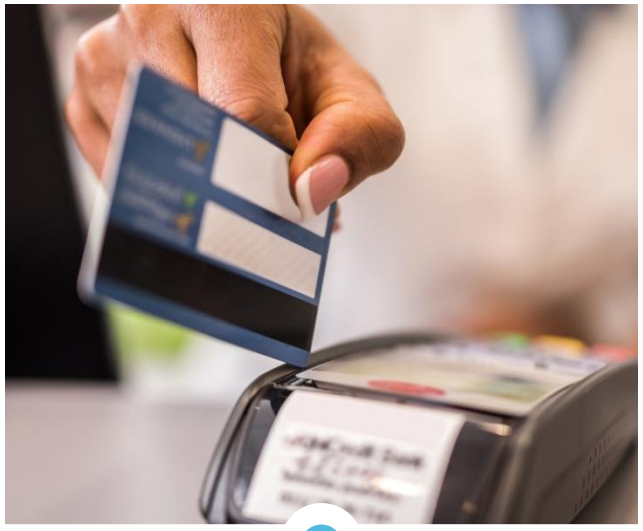
The fourth payments revolution

Ilustrative

Analog

The First Revolution

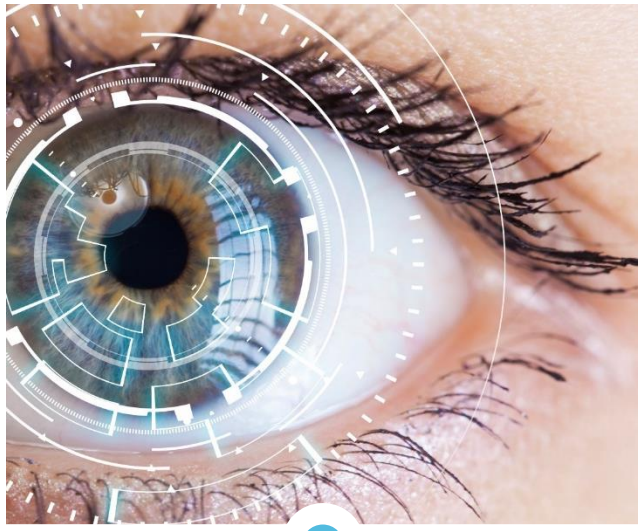
Introduction of the payment card

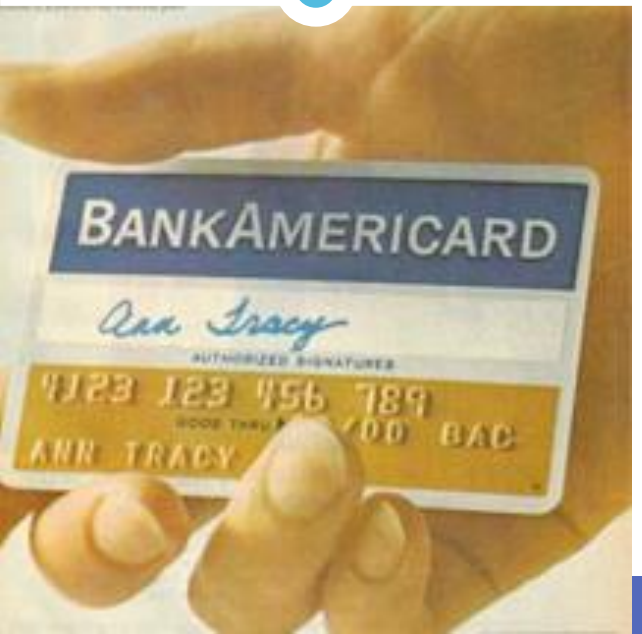


Digital

The Third Revolution

Tokenization and enhanced data

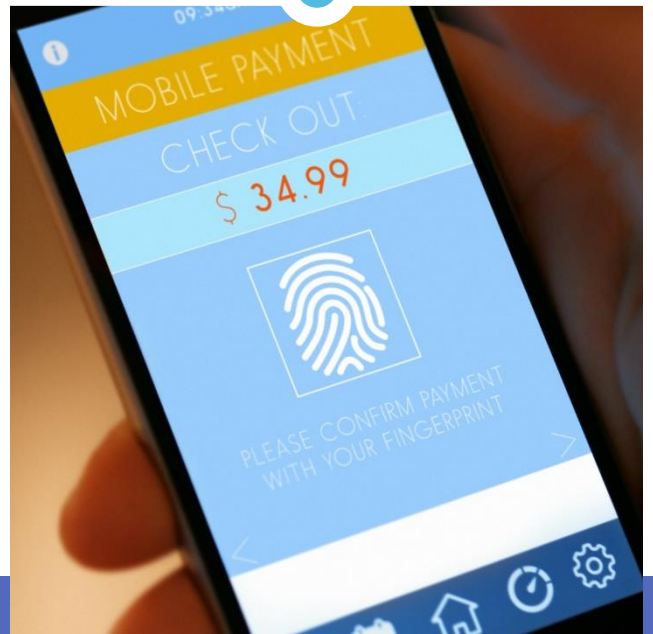




Electronic

The Second Revolution

Magnetic and chip cards



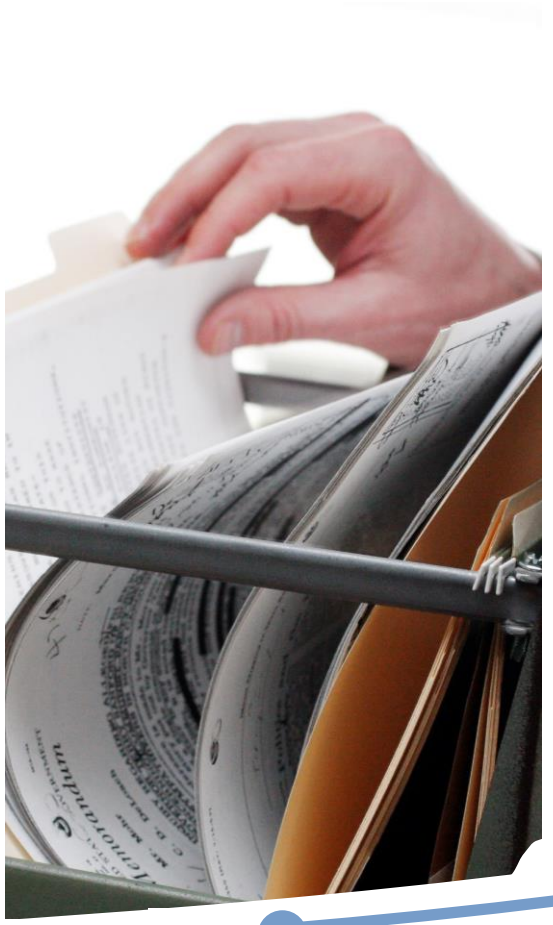
Near future

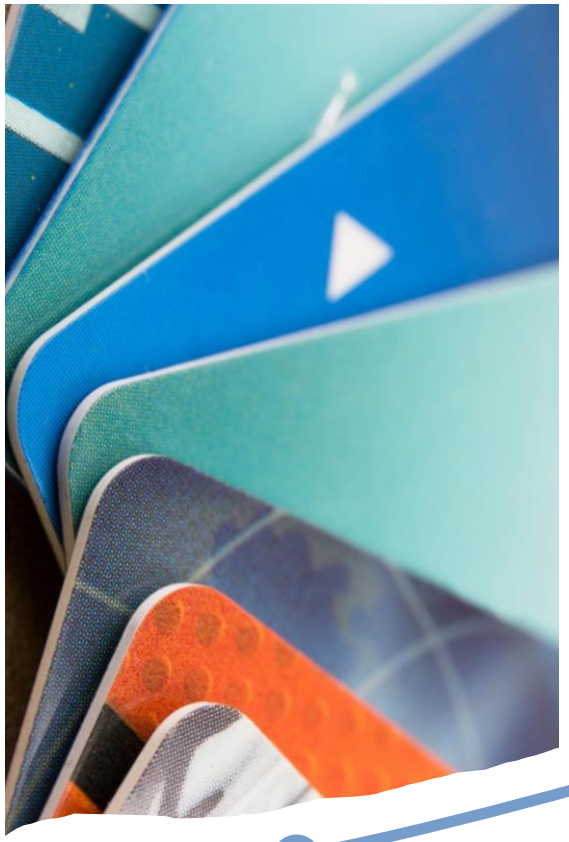
The Fourth Revolution

Emerging technologies (Quantum Computing, AI, IOT, Biometrics)

The evolving nature of fraud

Fraud scope





The First Revolution
Dumpster diving

The Second Revolution
Stolen & counterfeit cards

The Third Revolution
Mass data breaches

The Fourth Revolution
Emerging threat vectors

Ilustrative

Small Businesses

- Large population (~5MM+)
- Low/no security controls

Actionable Items

- Implement secure technology – EMV chip, P2PE, tokenization
- Perform security basics: password management, patching systems /

Integrators & Resellers

- Frequently targeted by hackers
- Improper Point-of-Sale (POS) implementation
- Always-on remote access connectivity
- Common username / passwords

Actionable Items

Hospitality Industry

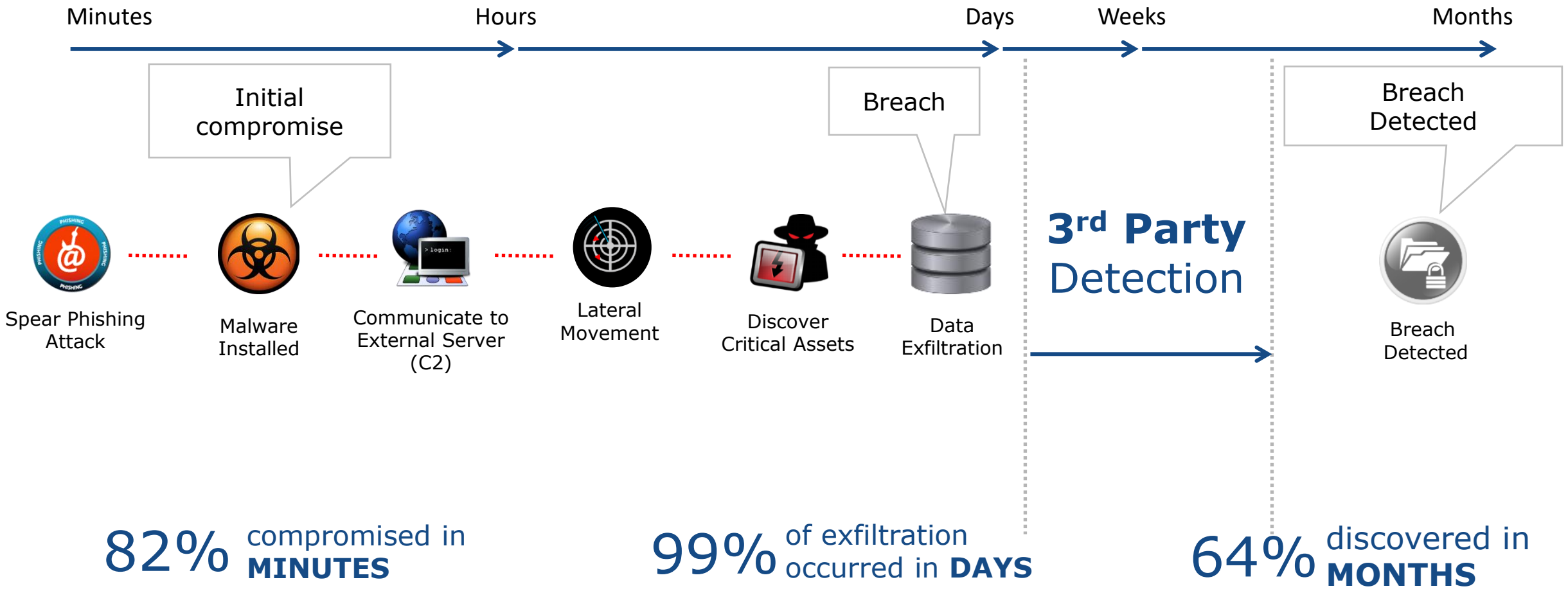
- Increased focus on hotels and restaurants
- Typically, back of house servers or property management systems
- Common breach methods include social engineering or spear phishing attacks
- Malware on systems allows attackers

Who are the Targets?

Hackers and Fraudsters target specific industries and victims

The Challenge for **The Merchant**

Attackers Quickly Turn Incidents into Breaches



82% compromised in **MINUTES**

99% of exfiltration occurred in **DAYS**

64% discovered in **MONTHS**

GAP OF GRIEF

SECURITY DETAIL

Account lockouts
Failed user access attempts
Web shell deletions
Buffer overflows
SQL injections
Cross-site scripting
Denial-of-service
IDS/IPS events
Incident level fixes

BUSINESS RISK

How bad is it?
Who was it?
How did they get in?
What information was taken?
What are the legal implications?
Is it under control?
What are the damages?
What do we tell people?

Cybercrime Pandemic

2020 In Review: Mass Digitalization Spurs on Fraud

Cybercrime Pandemic

What Changed in 2020?

The Digitized World

With much of the world stuck inside for large parts of the year, people turned to digital channels for everything from shopping to gaming to streaming media and more. In fact, the Arkose Labs network saw 4 times as many transactions overall compared to the prior year.

The Changing Face Of Fraud

As noted earlier, socio-economic factors brought on by Covid-19 forced many typically law-abiding citizens into fraud to make ends meet. There was also an onslaught of chargebacks, as consumers canceled trips and demanded refunds for orders taking too long to ship.

A Stress Test Of Fraud Systems

The massive spike in digital traffic to online platforms, made for something of an unexpected stress test for fraud systems. Suddenly, old models of what suspicious behavior looked like were thrown out the window, and for many platforms daily traffic was at rates normally only reserved for the business times of year.

The New Home Office

The switch to remote working spurred a much-needed digital transformation for internal fraud and security teams. Many realized that large teams were no longer required to be on-site, and servers could be monitored and even power switches turned on and off remotely.

New Attack Types

2020 saw a rise in hybrid attacks, as bots were used to launch many large scale/low reward attacks that relied on brute force, with humans supplementing attacks in which more nuance was required. Account takeover attacks in particular spiked, as fraudsters targeted the wealth of new accounts created by consumers using digital services for the first time.

Cybercrime Pandemic

2020 End of the Year Survey: Insights from the Field

Stimulus Fraud

Stimulus checks provided a new way to make instant cash, with an influx of fake or stolen identities were created to open new fake accounts and gain unemployment checks.

Friendly Fraud

There was an alarming increase in the amount of friendly fraud, with people disputing genuine transactions, fueling a spate of more organized refund fraud attempts.

Human Click-Farms

There was a spike in human click-farms, as jobless people and those stuck to their homes looked for opportunities to earn money, regardless of where it came from.

New Avenues

As the number of new digital users swelled, fraudsters found a larger window of opportunity. From price gouging to delivery scams—especially masks and sanitizers—fraud rings milked every opportunity to monetize attacks.

Phishing & Social Engineering

Fraudsters used spam, social media, and social engineering techniques to play on the panic around COVID-19 to trick users into sharing their passwords. They even targeted labs creating vaccines for COVID-19 with ransomware.

Synthetic Identity

The shift to cash to CNP caused businesses to relook at authorization, fraud models and how to manage identities, especially in the wake of fraudsters increasingly using synthetic identities.

Key Risks

Digital transformations tend to affect nearly every facet of a business: strategy, ops, tech, process and people

6 key risk areas to consider for E-Commerce businesses

Cybersecurity *
Financial losses, disruption, or reputational damage as a consequence of unauthorized access or attacks on information technology systems (hardware, software, networks)

Payments *
Risks across various payment elements (customer onboarding, checkout flow, authorization, recurring payments, refunds, disputes, third party management, etc.)

Operations & Technology *
Failures in process, planning, and practices may lead to financial, time, or reputational impact – and in some cases disruption of business continuity.

Brand & Regulatory Compliance *
Violating brand rules or regulations can result in penalties, audits, or termination. Often related to deficient operational practices.

Legal
Expenses, losses, or business disruption as a consequence of legal dispute(s). May result from new regulations, lack of familiarity or preparation.

Reputational
Losses resulting from declining customer confidence. May result if business practices are perceived to be inadequate, dishonest, or incompetent.

* GM Sectec offers support in these areas

Immediate Actions

Short-term activities for E-Commerce merchants

Ensure PCI compliance and regular third-party reviews

Evaluate data from multiple sources to better recognize and block unusual customer payment behavior

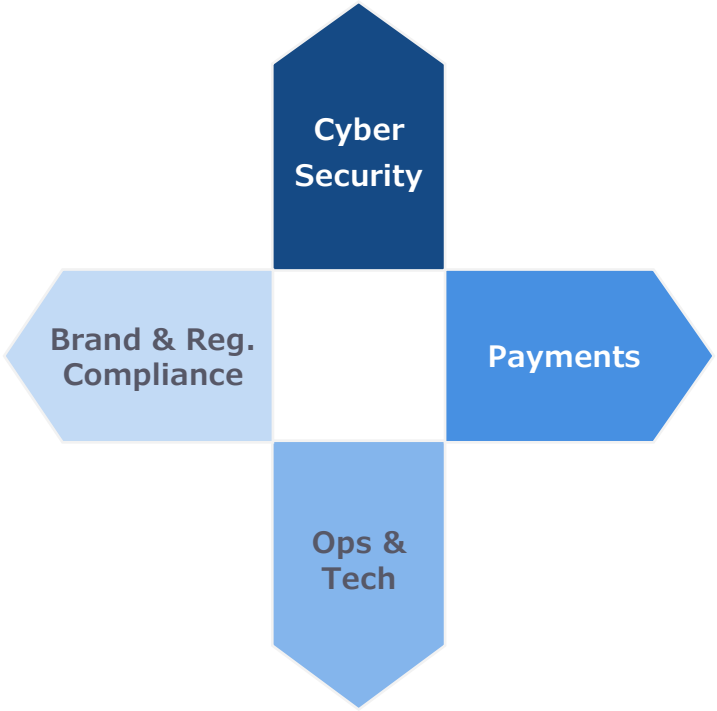
Make sure customers know what they are paying for at checkout and in the future

Immediate Actions

Short-term goals for E-Commerce merchants

Achieve PCI compliance; Require complex passwords and two-factor user authentication; Review data encryption practices; Ensure solid data breach response plan

Make sure customers know what they are paying (at time of checkout and in the future); Comply with consumer privacy and data protection regulations



Understand disputes, chargebacks, and authorizations; Evaluate acceptance of expanded online payment options

Review existing solution providers' capabilities to support post-pandemic business plans; Deliver consistent experiences across the customer journey (all channels and touch points)

GM sectec 50 YEARS

WWW.GMSECTEC.COM

OFFERING SERVICES

CLIENTS IN OVER
50 COUNTRIES

GLOBAL PRESENCE

OVER
50 THOUSAND
CLIENTS ENROLLED

GROWING

WITH MORE THAN
3 THOUSAND
SECURITY PROFESSIONALS

STRATEGIC ALLIANCE

WITH PR SCIENCE,
TECHNOLOGY AND RESEARCH
TRUST & POLYTECHNIC
UNIVERSITY OF PR

- SAN JUAN
- PANAMA CITY
- FT. LAUDERDALE
- MEXICO CITY
- SAO PAULO
- SANTIAGO
- BOGOTA
- MADRID
- MELBOURNE

EFFICIENCY

CONTROL

CHOICE

PREFERRED PARTNER

VISA | GM sectec

PCI APPROVED SCANNING VENDOR
PCI QUALIFIED SECURITY ASSESSOR
PCI P2PE - QUALIFIED SECURITY ASSESSOR
PCI 3DS ASSESSOR
PCI PA-DSS QUALIFIED SECURITY ASSESSOR
PCI CARD PRODUCTION SECURITY ASSESSOR
PCI QUALIFIED PIN ASSESSOR
PCI PCI FORENSIC INVESTIGATOR
UL LISTED
FIRST