Compromise Is Not an Option:
Beat Criminals at Their Own Game Through People, Process, and Technology

A discussion about safeguarding information and proactively addressing potential threats to a municipality and the community it serves.

Presented to:

Date: December 8, 2022

TD TEAM AT WORK FOR YOU

Adrienne Terpak, CTP

Commercial Banking
Segment Manager

Mobile: (973) 452-1725

Email: Adrienne.Terpak@td.com

Keith Pike

Sr. Government Banking
Relationship Manager

Mobile: (603) 660-3719

Email: Keith.Pike@td.com

KEY AREAS OF FOCUS

FRAUD SITUATION

ORGANIZATIONS ARE UNDER ATTACK

HUMAN & TECH

STRENGTHENING YOUR DEFENSES

WHAT'S GOING ON

NEW METHODS & THREATS

PAYMENT TRENDS

AUTOMATE AND DIGITIZE SECURELY

KEY TAKE-AWAYS

TO PROTECT YOUR ASSETS

Fraud Situation

THE NEED FOR HEIGHTENED AWARENESS

Local Municipality

6-figure ransom to decrypt system data

Long-Term Care Facility

Several wire payments sent totaling 6 figures

Higher Education Institution

6-figure wire sent to a fraudulent "supplier"

All Types, All Sizes

Losses due to check, ACH, card, wire insider and external crimes

Criminal attacks are inevitable, data breaches and financial losses don't have to be.

WHAT'S GOING ON
YOU ARE A TARGET

DEMOCRATIZATION OF CRIME

Large or small; public, privately owned or a government municipality – it doesn't matter, you are at risk.

You ARE being surveilled

You ARE under attack

You ARE NOT flying under the radar

JUST A FEW OF THE PUBLICIZED CYBER ATTACKS IN 2021:

- JBS Foods
- The Steamship Authority of Massachusetts
- Colonial Pipeline
- Scripps
- Acer
- Illinois Attorney General's Office

CYBERCRIMINAL METHODOLOGY

TODAY'S CRIMINAL OPERATES DIFFERENTLY

PERSISTENT

Constantly adjusting their attack methods until they find an angle that is successful.

SOPHISTICATED

Attempts are increasingly more convincing and better executed with intricate technology.

TARGETED

Broad tactics are still being utilized, but activities are also being tailored to identify weaknesses and penetrate vulnerable organizations.

AUTOMATED

Use software to increase efficiency and effectiveness by continually probing targets and uncovering weaknesses.

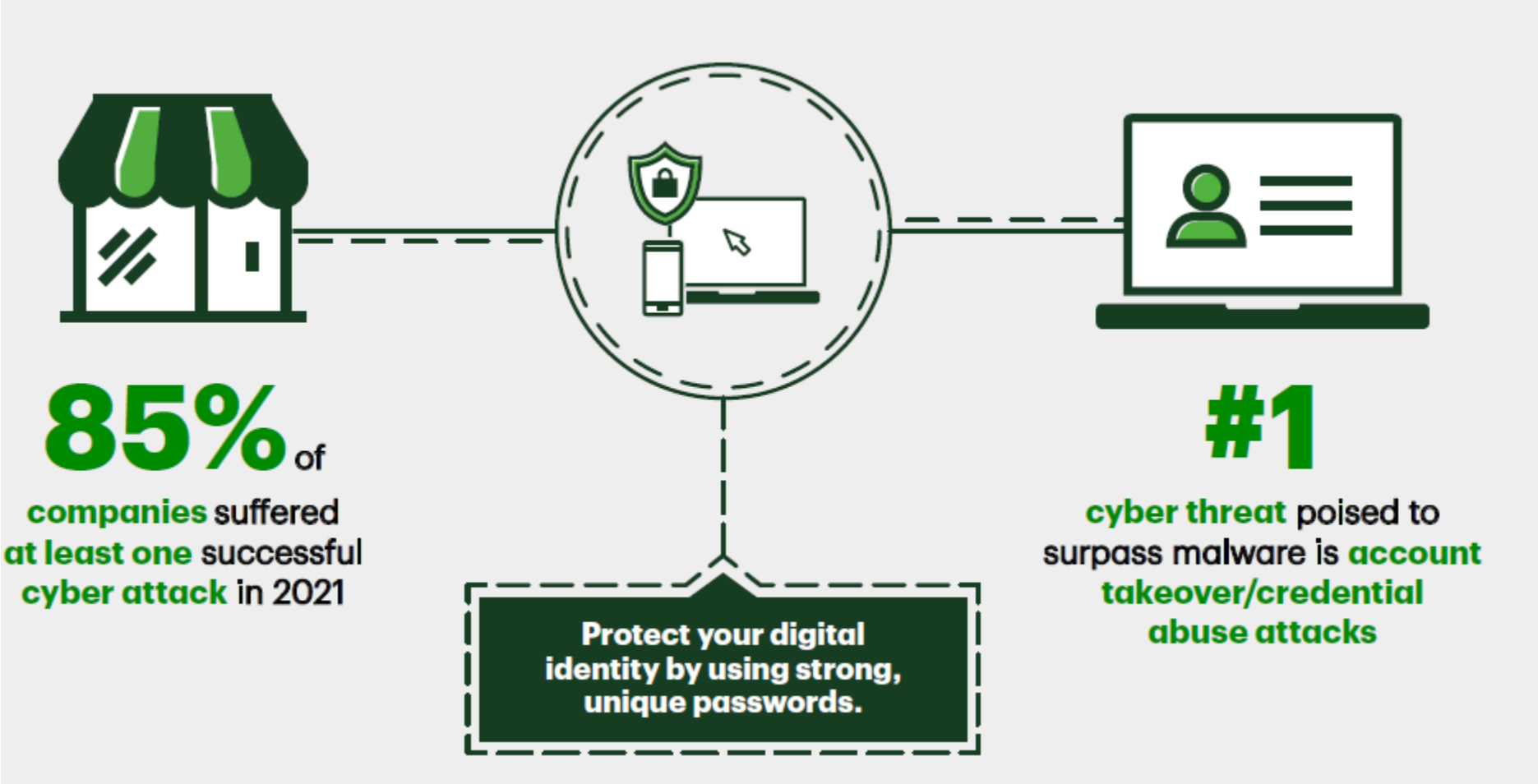
PATIENT

They will watch for the ideal time to strike and are willing to steal encrypted data today with the confidence that technological advances will allow for an eventual payout.

ADAPTIVE

They are not abandoning their tried-and-true methods, but they are consistently adding new methods and adjusting to be most effective.

Awareness and Prevention Start With You



Identity Theft and Account Takeover Fraud

A common form of identity theft, account takeover (ATO) fraud occurs when cybercriminals gain access to your online accounts and use them to withdraw money, make purchases, or extract information they can sell or use to access your other accounts.

Email, social media and bank accounts are potential ATO targets. Stolen user credentials can be purchased on the dark web following a data breach; they can also be obtained through phishing and malware attacks.

Stay Vigilant Against Persistent Threats

74% of organizations provide training on Business Email Compromise threats and how to identify phishing attempts

71% of businesses report being victims of payment fraud in 2021

~60% of organizations indicate Accounts Payable Departments are most vulnerable to Business Email Compromise scams

What You Can Do

The Human Firewall

Fraud awareness training for employees is highly effective in the fight against fraud — especially when coupled with knowledge assessments and repetition.

Be alert to scams and report them promptly

Use anti-virus software

Update software regularly

Use unique passwords for different accounts (bank apps, social media, email)

Cyber Hygiene Rule of Thumb:

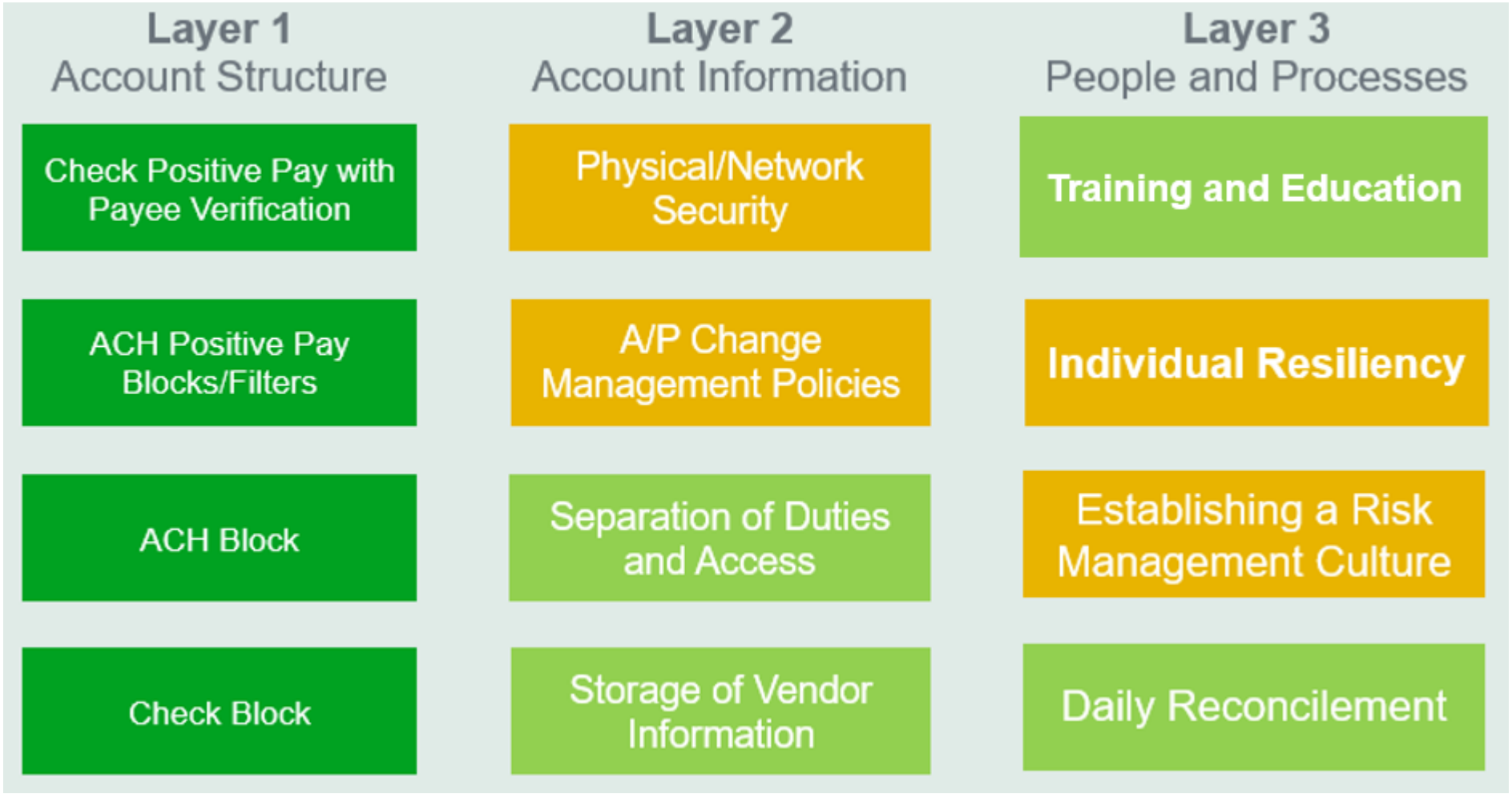
Avoid sharing sensitive data in emails, texts, and social media – criminals can use it to impersonate you!

Don't open attachments or click links from unknown senders

Never share account information or user credentials

Always verify payment instructions verbally with a trusted source

Fraud Mitigation Strategy



Legend

Bank-Offered Products/Services	Dual Bank / Customer Approach	Customer Process/Tactics

TAKEAWAYS

TO HELP PROTECT YOUR ORGANIZATION'S ASSETS

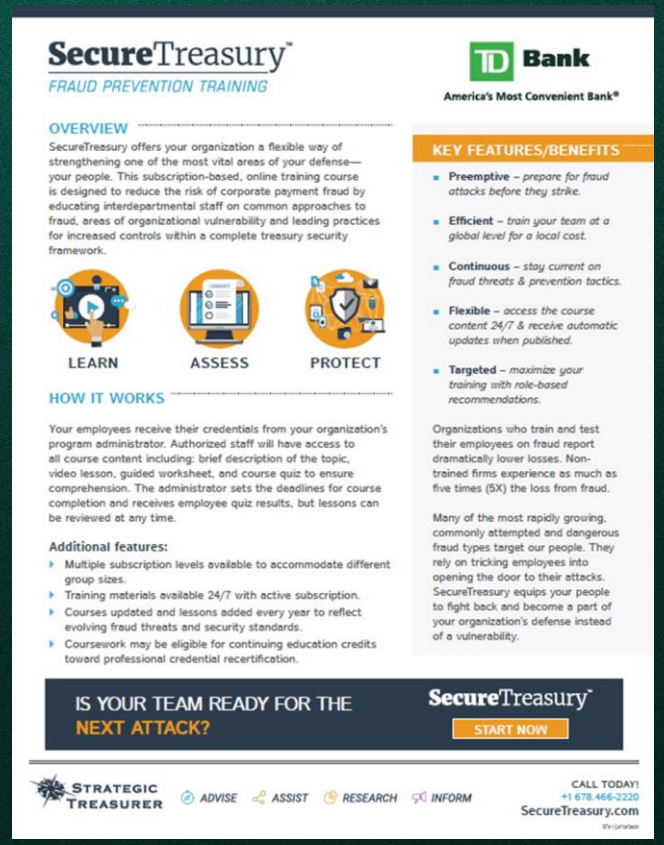
- THE BANK WILL NOT CALL/TEXT/EMAIL FOR YOUR CREDENTIALS
- DO PAYMENT SECURITY TRAINING & TESTING ANNUALLY
- STOP USING PUBLIC WI-FI AND UNSECURE EMAIL
- VERIFY THAT THE WEBSITE YOU ARE VISITING IS SECURE
- BOOKMARK BANKING SITES, DON'T RELY ON SEARCH
- PLAN FOR AN INCIDENT - STEPS TO TAKE, NUMBERS TO CALL

MORE TAKEAWAYS

TO HELP PROTECT YOUR ORGANIZATION'S ASSETS

- PUT BANK-OFFERED SECURITY SERVICES IN PLACE
- EVALUATE YOUR CYBER INSURANCE POLICY
- MAKE CYBER HYGIENE A PRIORITY FOR ALL ENDPOINTS
- DESIGNATE RESPONSIBILITY FOR FRAUD PREVENTION
- VERIFY ALL NEW INSTRUCTIONS VERBALLY WITH KNOWN CONTACTS
- BENCHMARK YOUR PRACTICES

ADDITIONAL RESOURCES AT YOUR FINGERTIPS



SecureTreasury™
FRAUD PREVENTION TRAINING

TD Bank
America's Most Convenient Bank®

OVERVIEW

SecureTreasury offers your organization a flexible way of strengthening one of the most vital areas of your defense—your people. This subscription-based, online training course is designed to reduce the risk of corporate payment fraud by educating interdepartmental staff on common approaches to fraud, areas of organizational vulnerability and leading practices for increased controls within a complete treasury security framework.

LEARN ASSESS PROTECT

HOW IT WORKS

Your employees receive their credentials from your organization's program administrator. Authorized staff will have access to all course content including: brief description of the topic, video lesson, guided worksheet, and course quiz to ensure comprehension. The administrator sets the deadlines for course completion and receives employee quiz results, but lessons can be reviewed at any time.

Additional features:

- Multiple subscription levels available to accommodate different group sizes.
- Training materials available 24/7 with active subscription.
- Courses updated and lessons added every year to reflect evolving fraud threats and security standards.
- Coursework may be eligible for continuing education credits toward professional credential recertification.

KEY FEATURES/BENEFITS

- **Preemptive** – *prepare for fraud attacks before they strike.*
- **Efficient** – *train your team at a global level for a local cost.*
- **Continuous** – *stay current on fraud threats & prevention tactics.*
- **Flexible** – *access the course content 24/7 & receive automatic updates when published.*
- **Targeted** – *maximize your training with role-based recommendations.*

Organizations who train and test their employees on fraud report dramatically lower losses. Non-trained firms experience as much as five times (5X) the loss from fraud.

Many of the most rapidly growing, commonly attempted and dangerous fraud types target our people. They rely on tricking employees into opening the door to their attacks. SecureTreasury equips your people to fight back and become a part of your organization's defense instead of a vulnerability.

IS YOUR TEAM READY FOR THE NEXT ATTACK?

SecureTreasury™
START NOW

STRATEGIC TREASURER ADVISE ASSIST RESEARCH INFORM

CALL TODAY!
+1 678.466-2220
SecureTreasury.com

TD Bank
Fraud Control
TD Commercial Banking Security Center

American Bankers Association (ABA)
banksneveraskthat.com

Cybersecurity & Infrastructure Security Agency
CISA Insights
CISA Cyber Hygiene Services

National Council of Information Sharing & Analysis Center (ISAC)
National ISACs

National Institute of Standards and Technology
NIST Cyber Framework

Strategic Treasurer
2022 Treasury Fraud & Controls Survey Report
SecureTreasury Fraud Prevention Training