Welcome

Cybersecurity and Your Bank: What You Need to Know

CALIBRE CPA GROUP
DECEMBER 13, 2023

Cybersecurity and Your Bank: What You Need to Know

DECEMBER 13, 2023

Protecting Your Organization from Fraud & Cyber threats

MICHAEL KELLEY| VP & INFORMATION SECURITY OFFICER
TRUIST FINANCIAL CORPORATION

THOMAS J. DEMAYO, CISSP CISA CIPP/US| PRINCIPAL
PKF O’CONNOR DAVIES, LLP

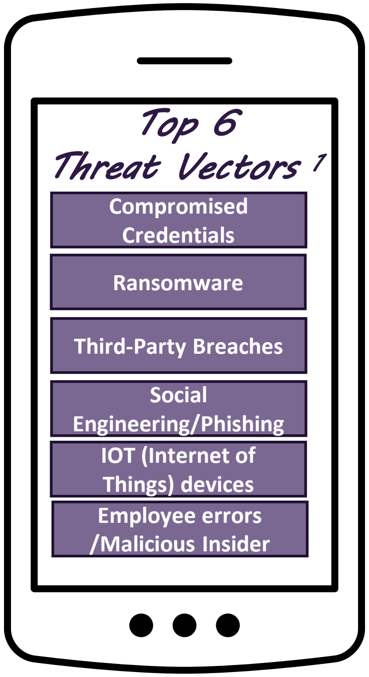
Protecting your organization from Fraud & Cyber threats

Wednesday, December 13th 2023

TRUIST

Table of Contents

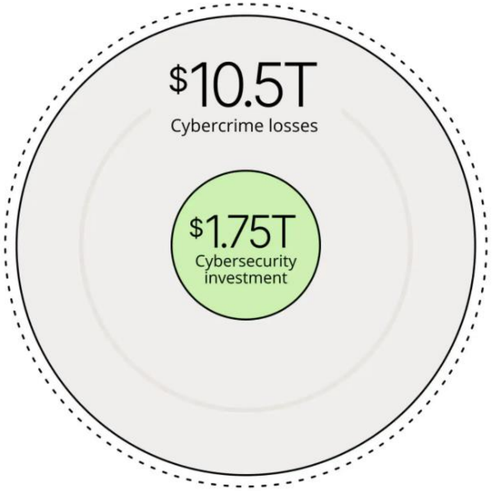
Cyber security industry perspective



Top 6 Threat Vectors [1]

- Compromised Credentials
- Ransomware
- Third-Party Breaches
- Social Engineering/Phishing
- IOT (Internet of Things) devices
- Employee errors /Malicious Insider

Top threat vectors cited[1]



2023 statistics[1-2]

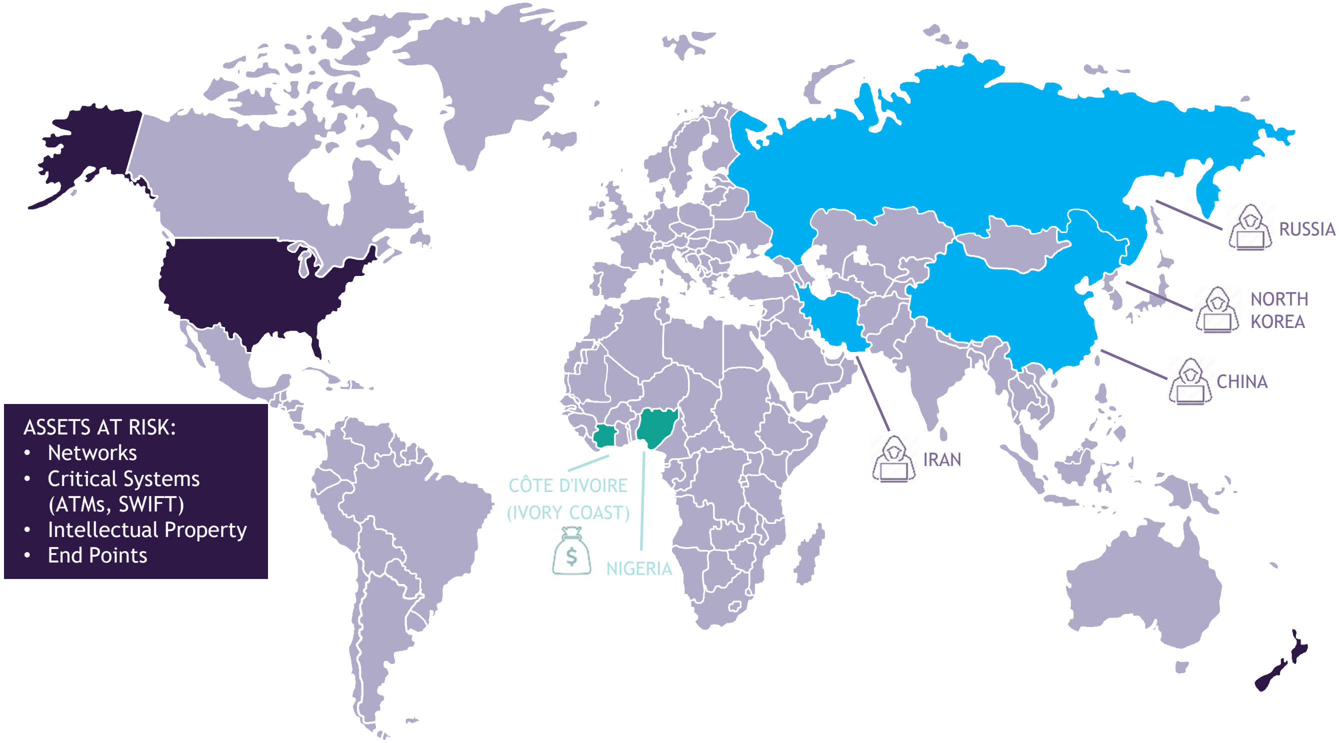
$4.45M[2]

Average cost of a data breach was at an all-time high across all sectors 15.3% increase since 2020

Sources: [1] 2022 Verizon DBIR report, [2] IBM Security's 2023 **Cost of a Data Breach Report**.

CYBER SECURITY RISKS

THREATS TO ORGANIZATIONS CONTINUES TO EVOLVE



ASSETS AT RISK:
- Networks
- Critical Systems (ATMs, SWIFT)
- Intellectual Property
- End Points

NATION STATES:
- Theft
- Espionage
- Disruption
- Regime Security

CAPABILITIES:
- DDoS
- Phishing-as-a-service (PhaaS) using AI/Fraud GPT
- Malware (ATM Jackpotting, Data Wiping, etc.)
- Third Party Compromise
- Global Network

CRIME SYNDICATES:
- Theft

CAPABILITIES:
- Business Email Compromise
- Social Engineering

SOURCE: IBM Think 2019, *How Financial Services Companies Should Respond to Cyber Security Attacks*

01

Train your employees as your first line of defense: Online Presence Awareness

TRUIST

Start with online presence awareness.

Are you and your staff oversharing?

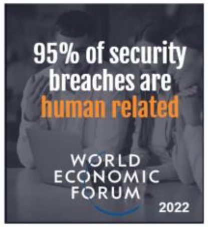
- Configure the privacy and security settings for information sharing when you:
  - Sign up for a new account
  - Download a new app
  - Get a new device
- Review settings regularly (at least once a year).

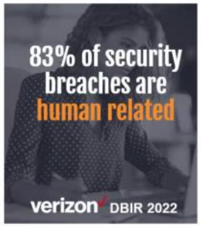
Share with care

- Think before posting. What does a post reveal? Who might see it? How might it affect you or others?

How can your data be used for fraud?

- Target profiling & identification (key company personnel, person with access to funds/data, job postings)
- Personalization of social engineering attacks (phishing, vishing, business email compromise)
- Extortion related to embarrassing content (photos, comments)
- Identify theft (creation of bank accounts, mail accounts, or false identities for criminals)





Watch out for phishing and quishing

What is it?

Phishing is a form of social engineering using email or text to lure the recipient into providing confidential information like your passwords, account numbers, or Social Security numbers.

When in doubt, throw it out

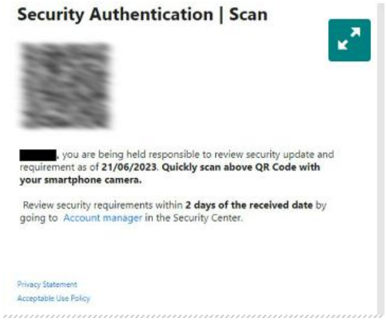
Why do attackers use phishing and quishing?

Phishing emails may look like they're from a company you know or trust—like the IRS, a financial institution, a social networking site, an online payment website, QR CODE or app, or an online store.

How to identify a phishing attempt

Phishing messages often convey **a sense of urgency** or **threats of dire consequences** to trick you into clicking on a link, opening an attachment, or providing information. Watch for:

- ✓ Suspicious activity or log-in attempts
- ✓ Problems with your account or your payment information
- ✓ Requests to confirm personal information
- ✓ Fake invoices or links to make a payment
- ✓ Faster or inflated government refunds
- ✓ QR Code-Never scan a QR code from an unfamiliar source.
- ✓ Benefits enrollment



Security Authentication | Scan

[redacted], you are being held responsible to review security update and requirement as of **21/06/2023**. **Quickly scan above QR Code with your smartphone camera.**

Review security requirements within **2 days of the received date** by going to Account manager in the Security Center.

Privacy Statement
Acceptable Use Policy

Other signs

- Grammatical errors, typos, odd formatting
- Unexpected attachments (.exe, .zip, .html)
- Unusual email addresses, web links—hover over links (or long-press on a mobile device) to reveal the true destination.

Be alert for vishing and SMiShing.

What is it?

Vishing and SMiShing is a form of social engineering using phone calls, text messages or automated phone services. It is voice phishing with the intent to lure the recipient into providing confidential information.

Why do attackers use vishing and SMiShing?

Attackers want to provide more assurance to their target, increasing success rates of getting large amounts of money transferred or access to additional data.

How to identify a vishing and SMiShing attempt

- ✓ Don’t trust the number on the Caller ID display. Scammers can make it look like they are calling from any number and often tell victims to Google their number to confirm that it’s legitimate (part of the fraud).
- ✓ Don’t provide or update personal or account information, even if scammers claim your account is suspended or deactivated.
- ✓ Common scams: Tax audit, tax refund, tech support, Zelle/One Time Password (OTP)

What to do

- ✓ When in doubt, end the call and contact the organization directly using a published customer service hotline. For example: the phone number or email published on your card, statement, or app.

TRUIST

Password complexity and multi-factor authentication

Complex passwords and multi-factor authentication first line of defense

Cyber criminals use dictionaries of various languages, names, and linguistic patterns to crack passwords along with social engineering attacks.

Do

- ✓Pick a phrase you will remember (e.g., “Be present now”).
- ✓Include capitalization, abbreviation, spelling, numbers, and punctuation.
- ✓Lengthen passwords to increase strength; add prefixes or suffixes.

Don’t

- ✓Choose passwords based on personal details (e.g., mother’s maiden name, birth dates, family names, etc.).
- ✓Use the same password for multiple accounts.
- ✓Disclose your passwords online, give them to anyone, or store your passwords where they can easily be found.

Password	Time to Crack
Bepresentnow	Instantly
Be-Present-Now	>2 years
B3Pres3ntN0w2021!	>100 years

81 of confirmed breaches are related to stolen, weak, or reused passwords.

TRUIST

02

Set up adequate internal process controls

Create processes and controls to defend against fraud.

How organizations are defending themselves
Ways financial professionals are safeguarding their companies include:

85%
use payee name positive pay to verify the authenticity of checks

62%
segregate accounts

54%
perform daily reconciliation on ACH debit accounts

Questions to consider:

When did you last review your payments risk and policies?

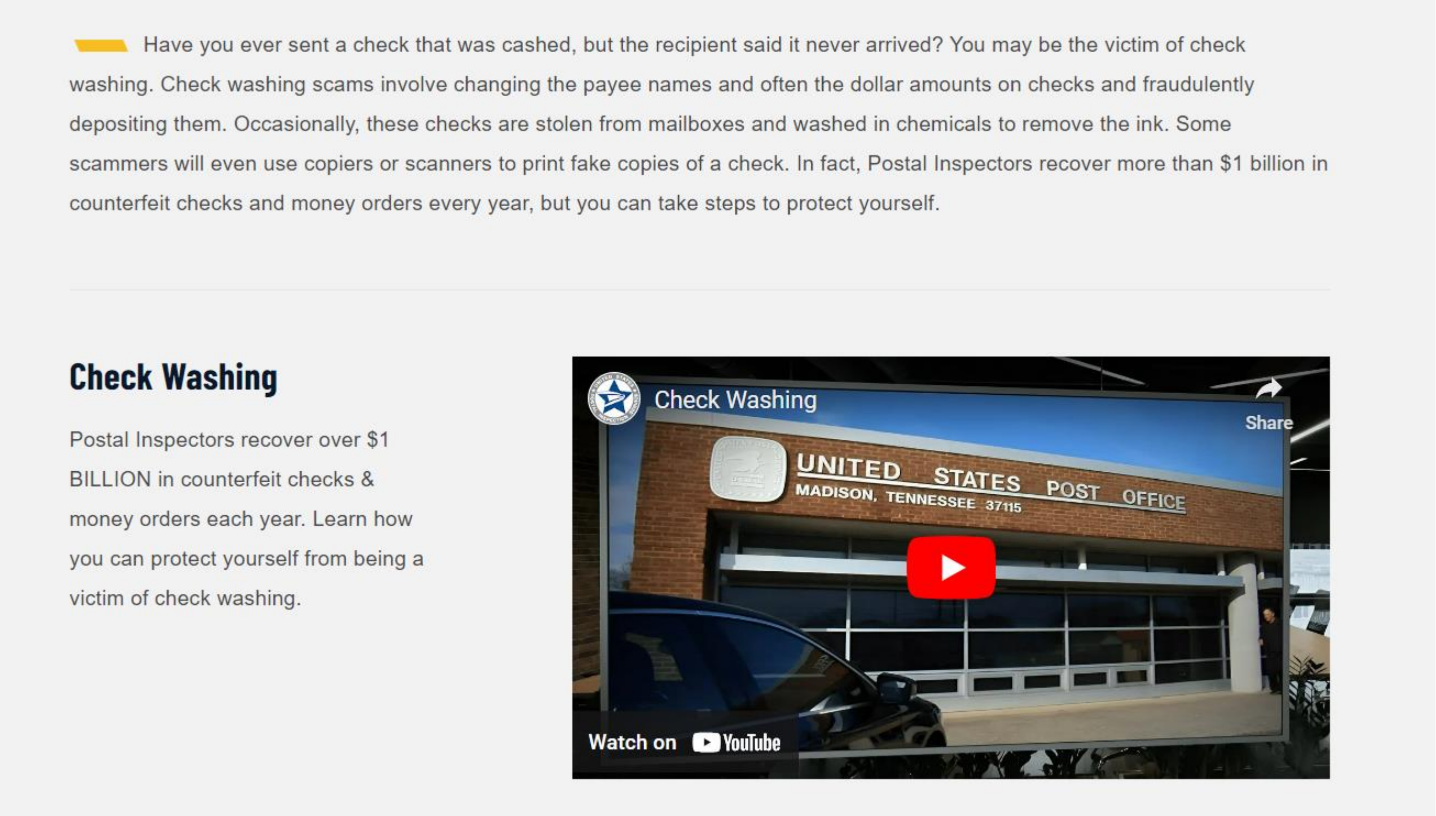
- Segregation of accounts – Keep separate accounts for business and personal so you can understand your business cash flow and profitability, reduce the risk of tax mistakes, and build credibility with bankers and investors.
- Daily reconciliation – Match activity showing on your financial system with transactions posted on your bank account.

Have you set restrictions on check and ACH debits?

- Block all ACH debits except on a single account set up with ACH debit filter/ACH positive pay.
- Organizations with high volumes of check payments should consider check protection with positive pay including payee name verification.

Source: 2021 AFP Payments Fraud and Control Survey.

USPIS Check Fraud



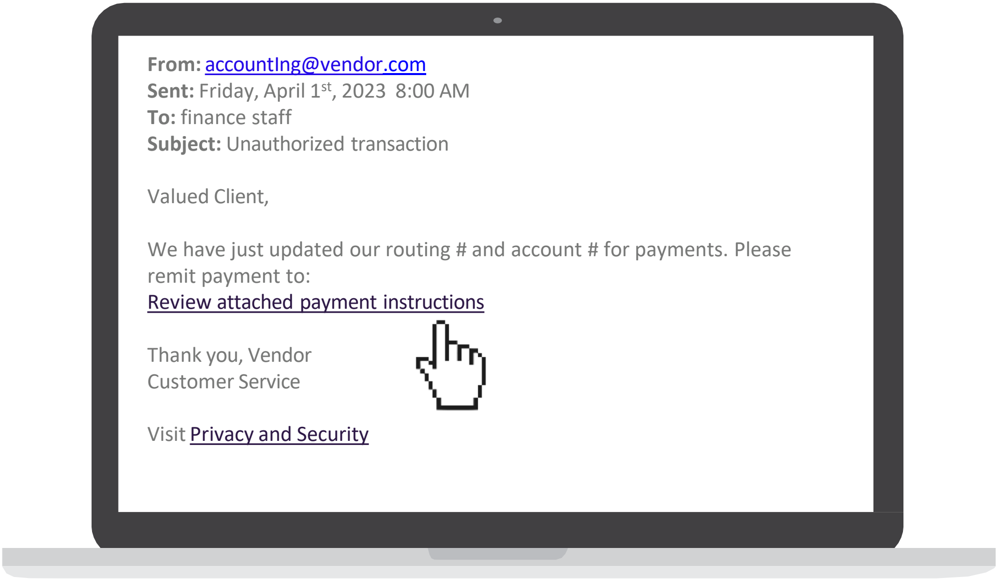
Have you ever sent a check that was cashed, but the recipient said it never arrived? You may be the victim of check washing. Check washing scams involve changing the payee names and often the dollar amounts on checks and fraudulently depositing them. Occasionally, these checks are stolen from mailboxes and washed in chemicals to remove the ink. Some scammers will even use copiers or scanners to print fake copies of a check. In fact, Postal Inspectors recover more than $1 billion in counterfeit checks and money orders every year, but you can take steps to protect yourself.

Check Washing

Postal Inspectors recover over $1 BILLION in counterfeit checks & money orders each year. Learn how you can protect yourself from being a victim of check washing.

Source: USPIS Check Washing 10-13-2023

Business/Vendor Email Compromise



From: accountIng@vendor.com
Sent: Friday, April 1st, 2023 8:00 AM
To: finance staff
Subject: Unauthorized transaction

Valued Client,

We have just updated our routing # and account # for payments. Please remit payment to:
Review attached payment instructions

Thank you, Vendor
Customer Service

Visit Privacy and Security

Thieves are now using AI deepfakes to trick companies into sending them money

$50B

IC3 report of total Business Email Compromise losses over the years 2013 to 2022

Source - https://www.ic3.gov/Media/Y2023/PSA230609 *Business Email Compromise: The $50 Billion Scam*

Best Practices to Mitigate ACH/Wire Fraud

WIRE/ACH

- Educate your staff about the fraud risks inherent in their daily processes. Training, training and more training!
- Create a culture that empowers employees to ask questions
- Develop processes for wire validation that include access to key executives for approval
- Require two people to approve the movement of large sums or to make changes to any information that impacts the movement of funds (establish a verbal passcode)
- Verify important or large transactions through an alternate method

VENDOR

- Train associates on all vendor management policies
- Empower employees to ask questions when in doubt
- Know your vendor
- Plan how your vendor will connect to you
- Validate changes to Vendor Master File
- Understand the vendors cybersecurity policies
- Require verbal confirmations
- New vendor system flags

03

Shore up your digital defenses

TRUIST

Strengthen your digital defenses.

- **Strengthen firewalls especially Remote Desktop Protocol (RDP).** Reduce risk of infection from ransomware and malware by configuring devices and software for automatic updates.
- **Establish data loss prevention and encrypt sensitive information.** Implement strong controls around the most sensitive data and ensure that data is encrypted at rest and in motion.
- **Limit device access to authorized individuals.** Laptops can be easy targets for theft or loss—lock them when unattended. Use a separate user account for each employee and require strong passwords. Restrict administrative privileges to trusted IT staff and key personnel.
- **Utilize multi-factor authentication (MFA) wherever it’s available.**
- **Regularly back up the data on all computers.** Back up data automatically if possible, or at least weekly, and utilize a cloud service or store copies offsite.

Remote work means more mobile solutions to protect.

- **Internet of Things (IOT)** – Limit what you connect to the network. Smart speakers make a convenient device hub but educate employees on turning off listening devices during work hours which creates additional privacy and security risks.
- **Encourage staff to establish a strong password** on their home routers and educate your staff on the risks of public Wi-Fi when using email and financial services. Utilize a VPN (Virtual Private Network) especially if using public Wi-Fi networks.
- **Mobile device fraud protection is straightforward** – Basic measures such as encryption, password protection, and a clear policy for reporting lost or stolen devices can make the core of a strong mobile device defense strategy.

04

Have a proactive strategy for your financial accounts

TRUIST

Have a proactive cyber risk strategy for your organization.

Tips for mitigating cyber risk

1. Focus on cyber resiliency
2. Know your ‘Crown Jewels’
3. Apply a business lens
4. Have a plan
5. Measure effectiveness
6. Make security everyone’s responsibility
7. Know when to contact partners and law enforcement

“Aligning security with the business goes beyond traditional methods of justifying security spend, such as warning of consequences from hacks or trying to prove ROI.”

Source: Why IT leaders are putting more business spin on security spend

Truist Fraud Protection and Prevention Solutions

Check Block

When the client has an account that will have no check disbursements (for example zero balance account) and wants to prevent check fraud on the account, a total block on check debits can be imposed. No action is needed on the part of the client (no issue file, no notifications); all checks are returned the next business day.

Cyber Risk Insurance

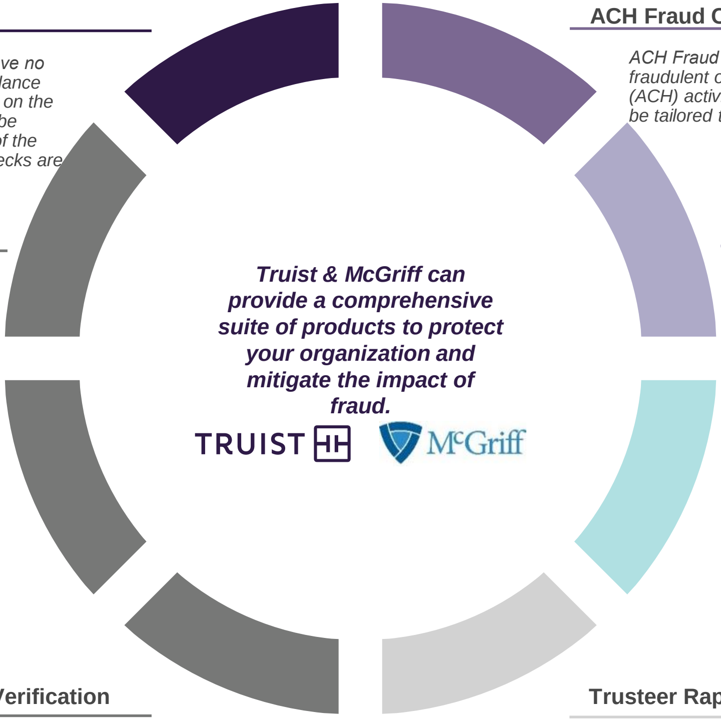
To help your organization respond and recover from network and information security breaches, McGriff's experienced specialists can strategically develop insurance coverage tailored to your company's risk profile and specific objectives

Universal Payment Identification Code

Maintains the privacy of your sensitive banking information by providing a permanent and secure account number alias that can be widely distributed to your trading partners.

Positive Pay with Payee Name Verification

Positive Pay safeguards client accounts by detecting suspicious checks and returning them. Positive Pay flags mismatching checks as exceptions and prompts the client to make a pay or return decision through their digital platform.



Truist & McGriff can provide a comprehensive suite of products to protect your organization and mitigate the impact of fraud.

TRUIST McGriff

ACH Fraud Control

ACH Fraud Control safeguards client accounts from fraudulent or unauthorized automated clearinghouse (ACH) activity. It offers multiple service options that can be tailored to meet the client's needs.

Controlled Disbursement Account

For companies with complex check disbursement requirements, Controlled Disbursement service simplifies daily funding decisions by providing a report every morning of the checks that will clear that evening.

Controlled Payment Reconciliation

Controlled Payment Reconciliation provides same day notification of suspicious checks along with daily disbursement reconciliation and funding information.

Trusteer Rapport

Trusteer Rapport is a security software application that is specifically designed to protect your company from browser-based fraud when you connect to websites containing sensitive information.

The security of client data is our highest priority

- Truist is one of the **largest** and most **financially sound** financial institutions in the country, and protecting our clients' confidential information is a top priority.

Our strategy includes:

- Engaging our board of directors, executive management, senior leadership, and a robust governance network in a **holistic** cybersecurity strategy.
- Participating in **industry trade organizations**, federal agencies and industry partners including the FBI, Department of Treasury, Homeland Security, Financial Services Information Sharing and Analysis Center (FS-ISAC), Cybersecurity and Infrastructure Security Agency (CISA), and others to develop and promote harmonized cybersecurity standards and best practices throughout the financial services sector
- **Continuous education to our teammates** on the latest cyber threats and scams to ensure they're equipped to recognize and respond appropriately to suspicious activity.
- **Cybersecurity Champions** program to educate hundreds of teammates across the footprint who in turn educate their peers to spread the word about cyber best practices to protect the organization and our clients.
- A comprehensive **array of security measures** in accordance with industry standards and regulatory requirements, and implementation of multiple layers of security and thousands of **highly skilled, dedicated teams** to safeguard client accounts and financial assets.
- **Proactively monitoring and detection** of cybercriminals and their capabilities and offering various **solutions** to help protect our clients from threats.
- **Ongoing client cybersecurity education** delivered through multiple print and digital channels. We encourage you to visit our fraud and security site on Truist.com where we offer helpful information to protect yourself and others from cyber-fraud and other scams.

TRUIST

Questions

Cybersecurity and Your Bank: What You Need to Know

CALIBRE CPA GROUP
DECEMBER 13, 2023