IDentityTheft 911
Protecting identities. Enhancing reputations.

Turn the Breach Around

The Positive Impact of Today’s Retail Breaches

Presented by:
Matthew Cullina
Chief Executive Officer
IDentity Theft 911

Company Overview

IDentityTheft 911
Protecting identities. Enhancing reputations.

Founded in 2003, IDentity Theft 911 is the nation's premier consultative provider of identity and data risk management, resolution and education services.

Our mission: As trusted partners we passionately serve our customers by first **listening**, then **advising**, **educating** and **advocating** to protect and restore their identities.

Leading Service Provider:

- Identity Management Solutions
- Identity Theft Recovery Services
- Fraud Monitoring Services
- Social Media Monitoring Services
- Commercial Data Breach Services
- Data Risk Management Services

Company Perspective

Our Partners trust IDentity Theft 911 because we:

600,000

Deliver data risk management services to more than 600,000 businesses.

Provide fraud resolution services to more than 17.5 million households.

Partner with insurance carriers, financial institutions and Fortune 500 companies.

Key Objectives

- How did this happen — An overview and timeline of the Target data breach
- Defining the problem — How the recent data breaches will impact your staff and members
- How you can help — Ways you can prepare and respond to breach incidents and turn incidents into member touch point opportunities.

The General Facts Around Target Breach

As it is currently understood

Target Breach Timeline

November 27th

- Probably first date of POS compromise by malware

December 2nd

- Payloads of stolen data transmitted to a hijacked website and then downloaded to a virtual private server in Russia from the FTP server
- This transfer of data continued approximately two weeks

Target Breach Timeline

IDentityTheft 911
Protecting identities. Enhancing reputations.

December 15th

- Target recognizes there is an *issue*
- Makes safeguarding their *environment* first priority

December 16th

- Investigation and forensic work initiated by Target

December 17th

- Target begins prepping its stores and call centers

> *By 6:00 at night, our environment was safe and secure. We eliminated the malware in the access points, so we were very confident that coming into Monday, guests could come to Target and shop with confidence at no risk.*

Gregg Steinhafel

President & CEO of Target Corporation

Target Breach Timeline

December 18th

- InfoSec blogger (Brian Krebs) posts initial report on the (as of yet) unannounced breach

December 19th

- Target releases first statement on their breach incident stating:

They are aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Approximately 40 million credit and debit card accounts may have been impacted between November 27 and December 15, 2013.

Target Breach Timeline

December 23rd

- FTC issues statement on its Blog warning of scams and fraudsters targeting Target shoppers
- Target announces that the DoJ is also investigating the data theft

December 24th

- Three separate class action lawsuits ALREADY filed against Target for the breach

December 27th

- Target confirms that (encrypted) PINs associated with the impacted payment cards were also exposed

1. If any email asks for your personal or financial information, it's most likely a scam
2. If there are links in the email, don't click on them, even if they seem legit at first glance

Target Breach Timeline

January 2nd

- East West Bank decides to reissue cards and sends announcement to customers

January 10th

- Target announces completely separate secondary data set on up to 70 million stolen in the breach, including:
  - Names
  - Addresses
  - E-mail
  - Phone number

Target Breach Timeline

January 12th

— Target CEO confirms to CNBC that attackers installed malware on POS devices

January 16th

— Malware known as POSRAM (similar to another piece of malware known as BlackPos) identified as the malware used

Target Breach Timeline

January 30th

- BMC Software issues statement around their widely used software and the fact that an .exe file named after one of their products, BUT not associated with it, may have been the way in

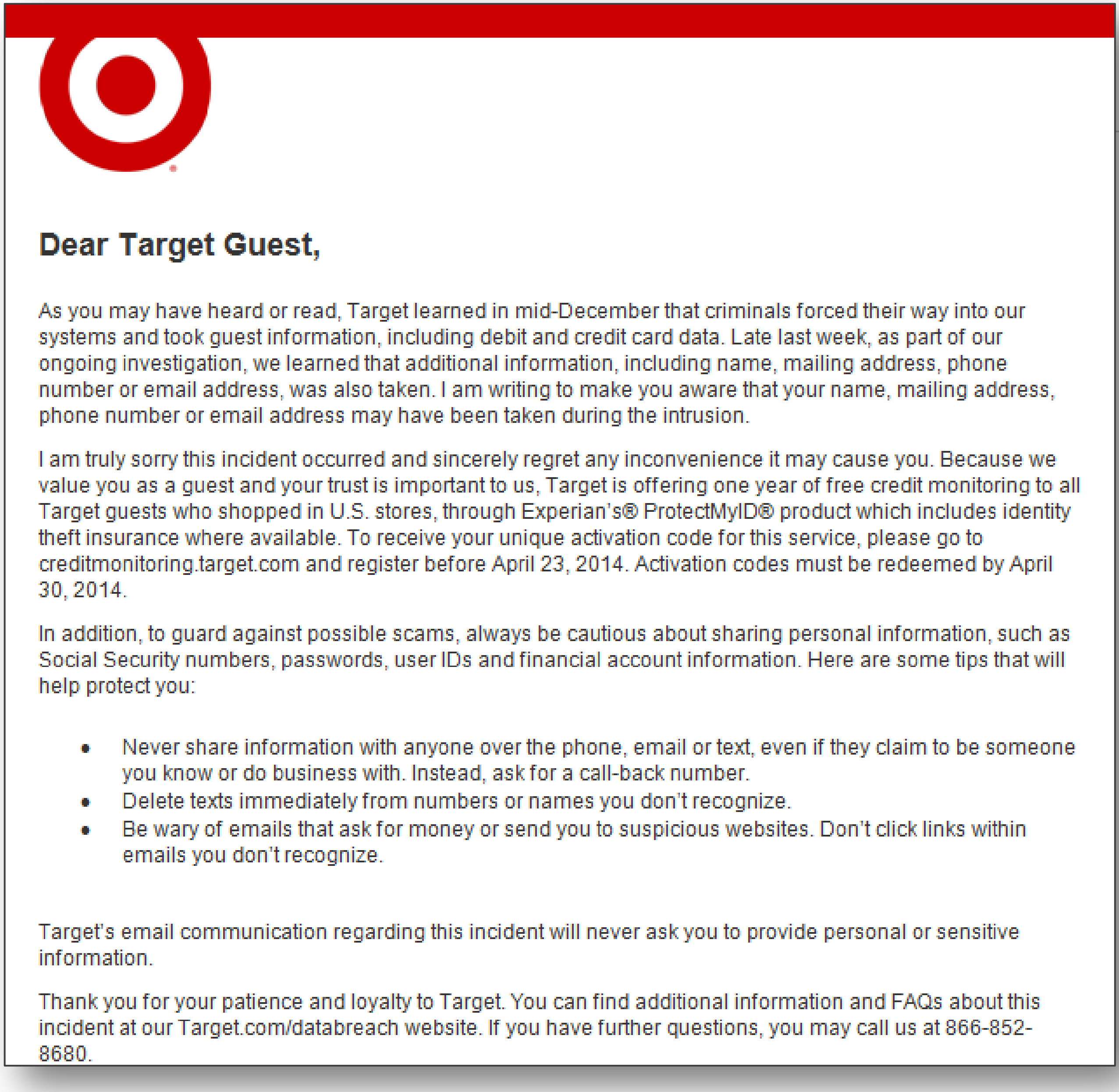
February 12th

- Revealed that a vendor, an HVAC firm, may have been the point of entry and the attack vector via the company's data connection to Target which was simply used for electronic billing, contract submission and project management

Scope of the Problem

Across the Retail Spectrum

Target Notification Email



Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website. If you have further questions, you may call us at 866-852-8680.

Poor Support and Communication

- Poor customer response by retailer (like Target) in large breaches, leaves Credit Unions to end up supporting the member when the retail solution is:
  - Inadequate from a customer support perspective
    - Retailer use of cheap and non-consumer friendly solution available will increase calls and concerns of CU Members to their FI
  - Ill fitting post breach solutions based on the facts and data lost have consumers following red herrings
    - Credit monitoring for a credit card breach poor solution that drives up issues at consumer FI's
    - No specificity of which card or cards were actually impacted means even more problems for CU's to support and more customer service inquiries

Possible Direct Costs to Credit Unions

- Notifying its members of issues related to the Target Data Breach
- Dedicating resources to provide customer support and guidance
- Closing out and opening new customer accounts
- Reissuing members’ cards ($10 per card)
- Refunding members’ losses resulting from the unauthorized use of their accounts or other related fraud
- Possible lost business due to fewer card transactions due to consumer fears resulting from exposures
- Fraud committed at Credit Union using stolen breach pii data

Wave of Class Action Lawsuits

- Multistate consumer lawsuits related to the holiday season Target data breach will be consolidated before U.S. District Court in St. Paul.
- The ruling of U.S. Judicial Panel brings together 33 lawsuits, filed in 18 districts, and more than 50 actions and potential "tag-along actions." The ruling cites actions in seven states, including Minnesota.
- Both consumer and business to business proceedings incorporated into consolidated action
- Several Banks and Credit Unions are plaintiffs seeking reimbursement for following costs:
  - Notifying its members of issues related to the Target Data Breach
  - Dedicating resources to provide customer support and guidance
  - Closing out and opening new customer accounts
  - Reissuing members’ cards ($10 per card)
  - Refunding members’ losses resulting from the unauthorized use of their accounts or other related fraud

Not Limited to Target, other recent breaches

AOL (April 2014)

- 2% of Users email data, passwords, contacts, security questions

Sallie Beauty Supplies (March 2014)

- 280k+ cards

Neiman Marcus (January 2014)

- 1.1 million cards

Yahoo (January 2014)

- Up to 81 million Yahoo passwords exposed

Michaels (January 2014)

- 3 million customer credit and debit card records

Adobe Systems (October 2013)

- 152 million names, credit & debit card numbers, & expiration dates

Where Creativity Happens®

Custom Attacks Can Be Outsourced

IDentityTheft 911
Protecting identities. Enhancing reputations.

Cost of the **Malware** written for the attack against Target cost between **$1800-$2200**

Ransomware prices can range from **$8-$25**

Trojans

- Keyloggers from **$3-$50**
- SMS Spyware from **$350**

Distributed Denial of Service Attack Services (Ddos)

- 1 hour = **$10**
- 1 day = **$30-$70**
- 1 week= **$150**
- 1 month= **$1200**

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Key Takeaways

Key Takeaways

- Communications around consumer data breaches are far from clear
- Solutions provided often do not fit the risk
- Notifications provided to consumers are often poor, misleading, confusing, and/or unclear
- Often, consumer oriented financial institutions like community banks, credit unions, etc. left to support those impacted by a 3rd party breach

Key Takeaways

Credit unions are often left with some of the clean up in the form of:

1. Service calls related to questions surrounding the breach

2. Inquiries from members/customers around what can be done to protect themselves

3. Panic calls regarding worries about fraud and identity theft

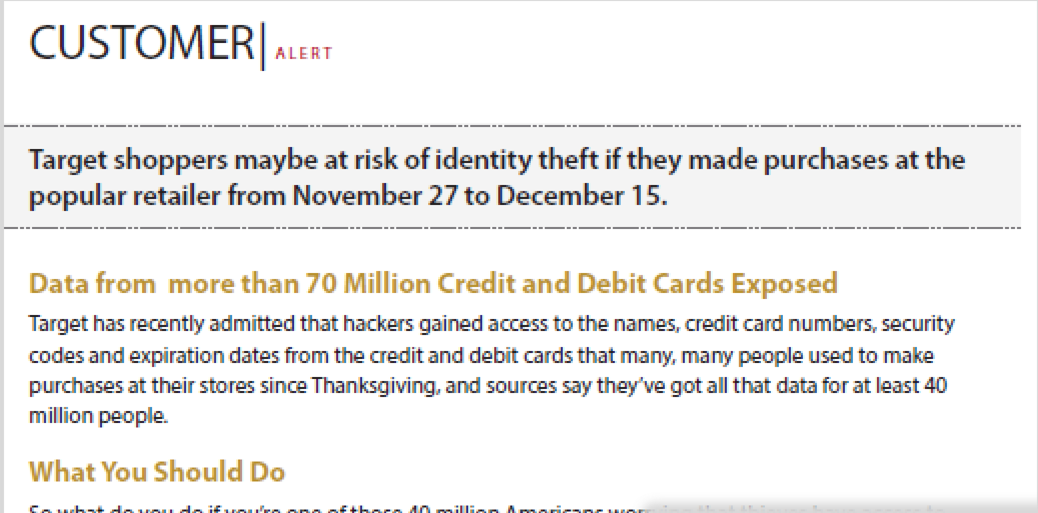
How Can You Help?

Before, During and After an Incident

Ways You Can Help

- Understand the details and ramifications of breaches when they happen
- Have an incident response plan ready for outside breaches with high potential to impact your members
- Educate member-facing staff so they are prepared to answer questions and advise about the real risks associated with a specific breach
- Offer 3rd Party Services to your customers or members to assist them in managing their identity before, during and after an incident
- Consider offering proactive monitoring solutions
- Turn negatives into positive member touch point opportunities

Communication is Key



CUSTOMER | ALERT

Target shoppers maybe at risk of identity theft if they made purchases at the popular retailer from November 27 to December 15.

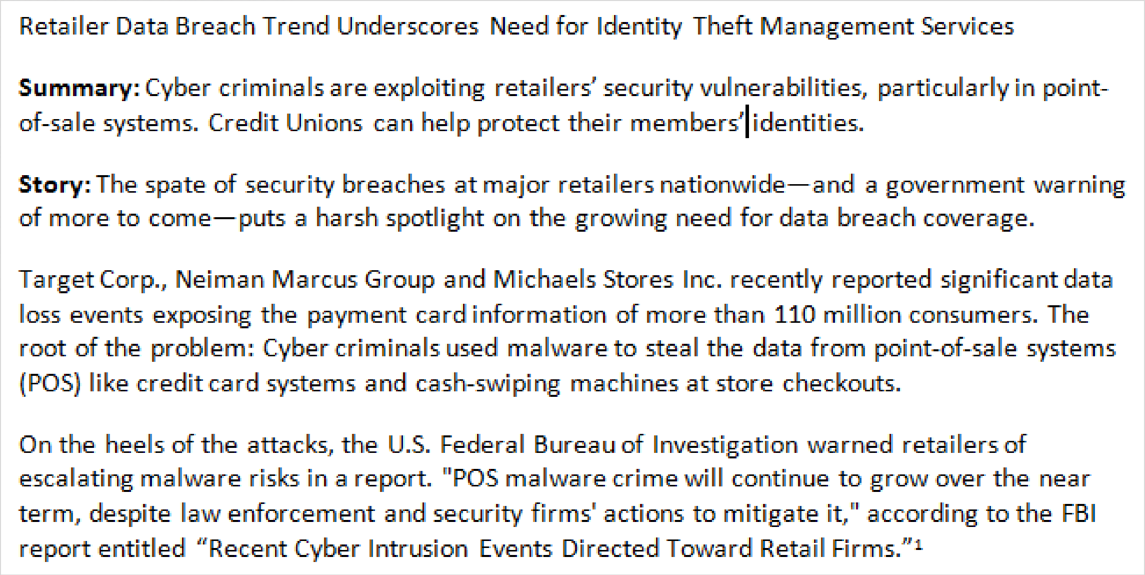
Data from more than 70 Million Credit and Debit Cards Exposed

Target has recently admitted that hackers gained access to the names, credit card numbers, security codes and expiration dates from the credit and debit cards that many, many people used to make purchases at their stores since Thanksgiving, and sources say they've got all that data for at least 40 million people.

What You Should Do

So what do you do if you're one of those 40 million Americans wor your credit or debit card information? Just follow these simple step shoulders just in time for the holidays.

1. **Check your account statements right now.** Use a secure online accounts and review credit card and bank account stat unfamiliar charges. Call your credit card issuer or bank.
2. **Replace your card ASAP.** The bad guys can recreate physic information and use them at any time. Even if they haven't us card has been compromised. Waiting to replace it may cost m trouble later.



Retailer Data Breach Trend Underscores Need for Identity Theft Management Services

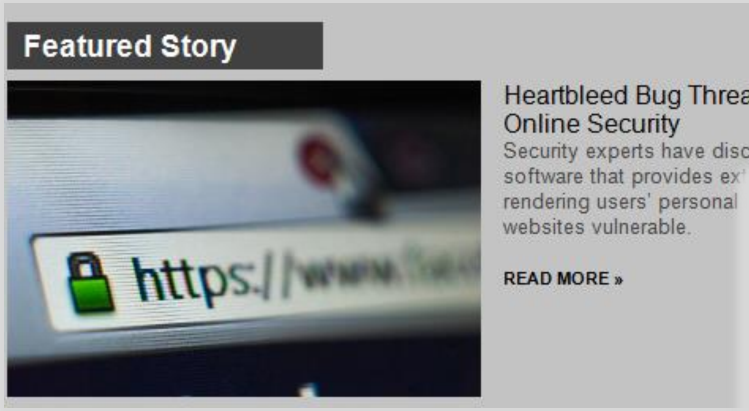
Summary: Cyber criminals are exploiting retailers' security vulnerabilities, particularly in point-of-sale systems. Credit Unions can help protect their members' identities.

Story: The spate of security breaches at major retailers nationwide—and a government warning of more to come—puts a harsh spotlight on the growing need for data breach coverage.

Target Corp., Neiman Marcus Group and Michaels Stores Inc. recently reported significant data loss events exposing the payment card information of more than 110 million consumers. The root of the problem: Cyber criminals used malware to steal the data from point-of-sale systems (POS) like credit card systems and cash-swiping machines at store checkouts.

On the heels of the attacks, the U.S. Federal Bureau of Investigation warned retailers of escalating malware risks in a report. "POS malware crime will continue to grow over the near term, despite law enforcement and security firms' actions to mitigate it," according to the FBI report entitled "Recent Cyber Intrusion Events Directed Toward Retail Firms."[1]

Financial Literacy in the Digital Age

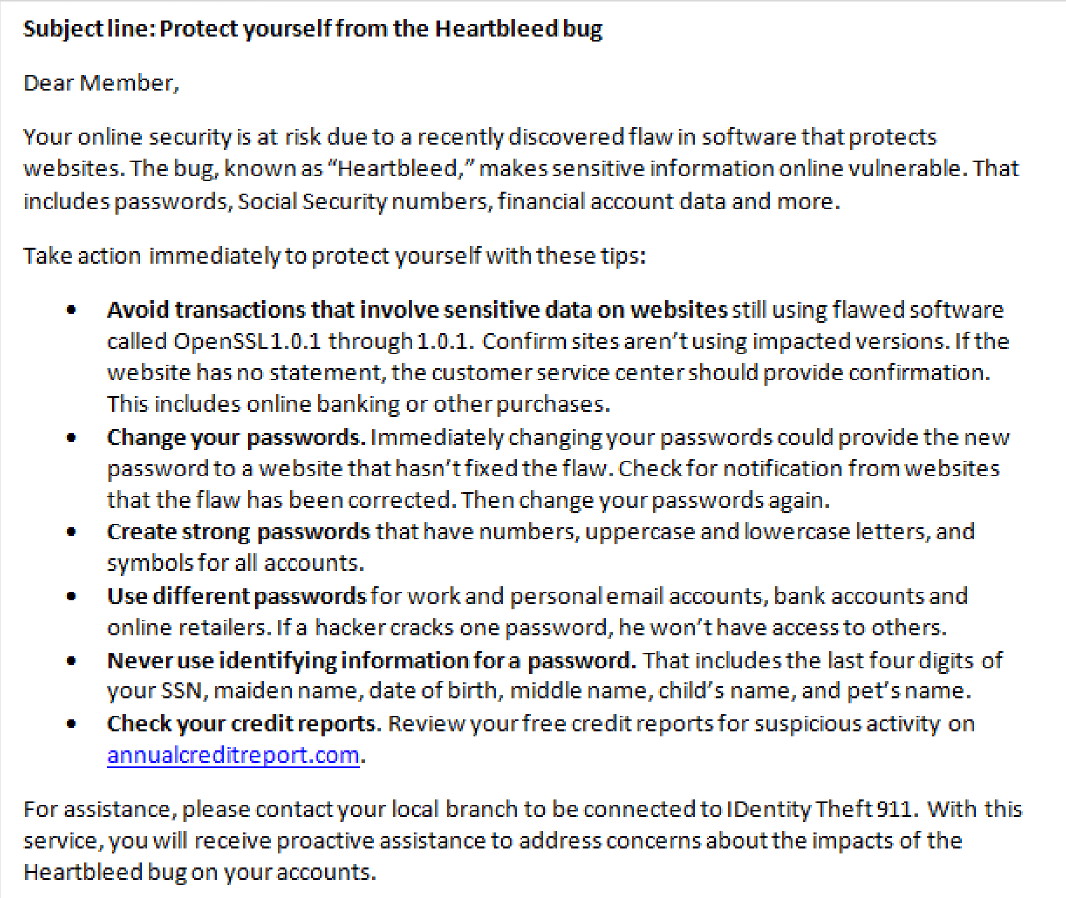


Featured Story

Heartbleed Bug Threatens Online Security

Security experts have discovered a flaw in the software that provides ex rendering users' personal websites vulnerable.

READ MORE »



Subject line: Protect yourself from the Heartbleed bug

Dear Member,

Your online security is at risk due to a recently discovered flaw in software that protects websites. The bug, known as "Heartbleed," makes sensitive information online vulnerable. That includes passwords, Social Security numbers, financial account data and more.

Take action immediately to protect yourself with these tips:

- **Avoid transactions that involve sensitive data on websites** still using flawed software called OpenSSL 1.0.1 through 1.0.1. Confirm sites aren't using impacted versions. If the website has no statement, the customer service center should provide confirmation. This includes online banking or other purchases.
- **Change your passwords.** Immediately changing your passwords could provide the new password to a website that hasn't fixed the flaw. Check for notification from websites that the flaw has been corrected. Then change your passwords again.
- **Create strong passwords** that have numbers, uppercase and lowercase letters, and symbols for all accounts.
- **Use different passwords** for work and personal email accounts, bank accounts and online retailers. If a hacker cracks one password, he won't have access to others.
- **Never use identifying information for a password.** That includes the last four digits of your SSN, maiden name, date of birth, middle name, child's name, and pet's name.
- **Check your credit reports.** Review your free credit reports for suspicious activity on annualcreditreport.com.

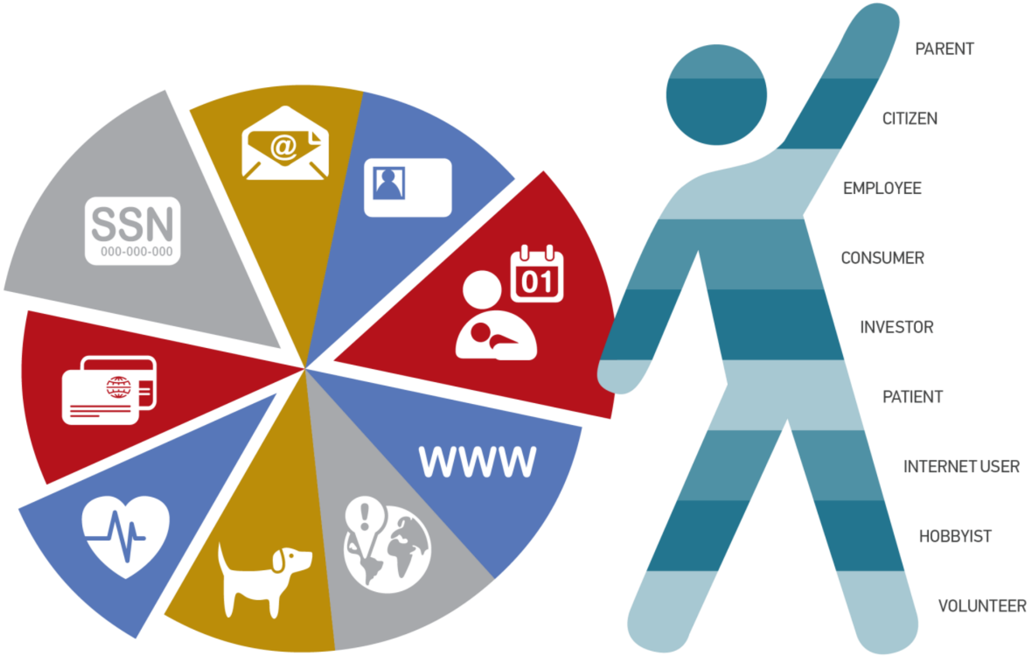
For assistance, please contact your local branch to be connected to IDentity Theft 911. With this service, you will receive proactive assistance to address concerns about the impacts of the Heartbleed bug on your accounts.

PII

YOUR PII CHART

LEGEND

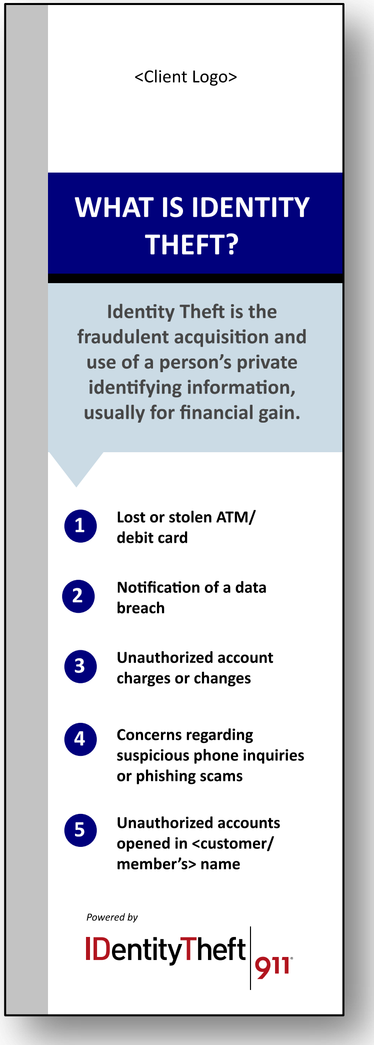
- SSN **SOCIAL SECURITY NUMBER**
- **CONTACT INFORMATION** (email address, physical address, telephone and mobile numbers)
- **GOVERNMENT-ISSUED IDENTIFICATION** (driver's license, passport, birth certificate, library card)
- **BIRTH DATE, BIRTH PLACE**
- WWW **ONLINE INFORMATION** (Facebook, social media, passwords, PINs)
- **GEOLOCATION** (smartphone, GPS, camera)
- **VERIFICATION DATA** (mother's maiden name, pets' and kids' names, high school, passwords)
- **MEDICAL RECORDS INFORMATION** (prescriptions, medical records, exams, images)
- **ACCOUNT NUMBERS** (bank, insurance, investments, credit cards)



Employee talking point guides

Talking Points & Action Monitor Card

- Frontline staff piece to help them identify trigger points of how to respond to member inquiries.
- Empowerment tool
- Action guideline



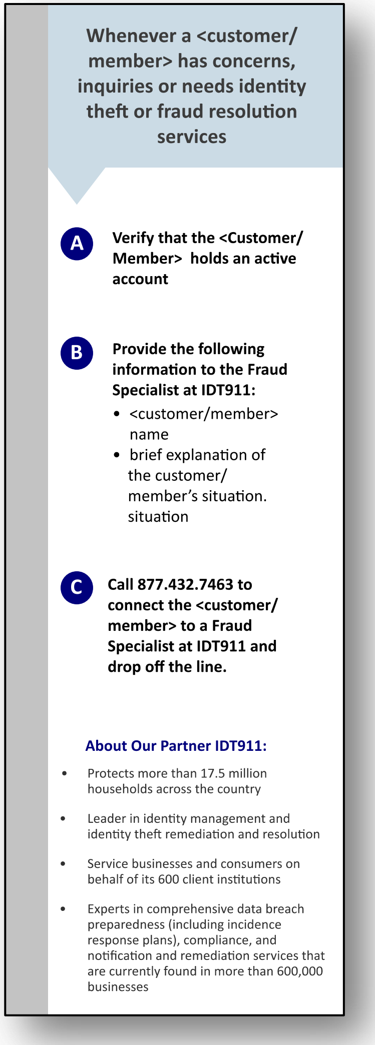
<Client Logo>

WHAT IS IDENTITY THEFT?

Identity Theft is the fraudulent acquisition and use of a person's private identifying information, usually for financial gain.

1. **Lost or stolen ATM/ debit card**
2. **Notification of a data breach**
3. **Unauthorized account charges or changes**
4. **Concerns regarding suspicious phone inquiries or phishing scams**
5. **Unauthorized accounts opened in <customer/ member's> name**

Powered by
IDentityTheft 911



Whenever a <customer/ member> has concerns, inquiries or needs identity theft or fraud resolution services

A **Verify that the <Customer/ Member> holds an active account**

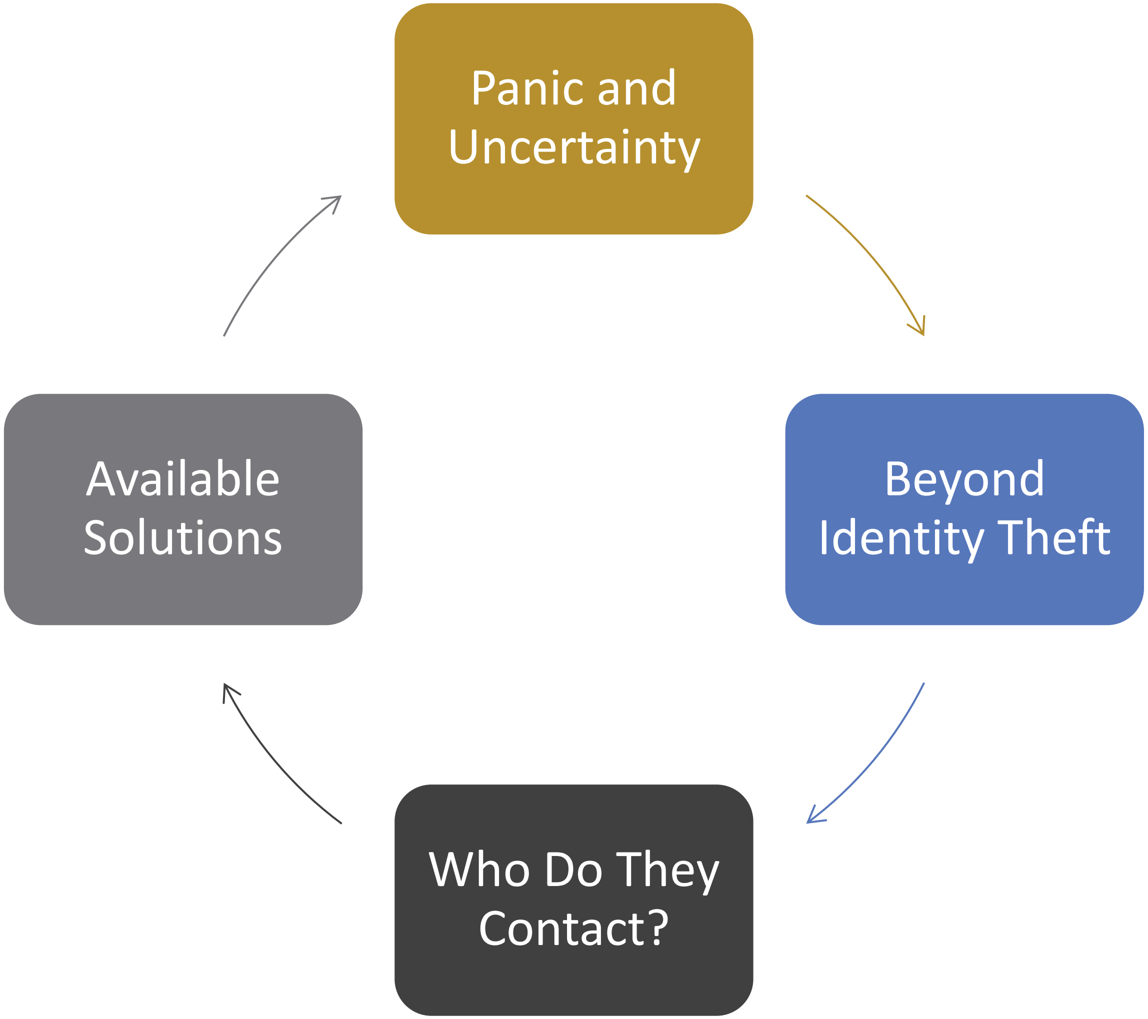
B **Provide the following information to the Fraud Specialist at IDT911:**
- <customer/member> name
- brief explanation of the customer/ member's situation. situation

C **Call 877.432.7463 to connect the <customer/ member> to a Fraud Specialist at IDT911 and drop off the line.**

About Our Partner IDT911:

- Protects more than 17.5 million households across the country
- Leader in identity management and identity theft remediation and resolution
- Service businesses and consumers on behalf of its 600 client institutions
- Experts in comprehensive data breach preparedness (including incidence response plans), compliance, and notification and remediation services that are currently found in more than 600,000 businesses

What to Expect



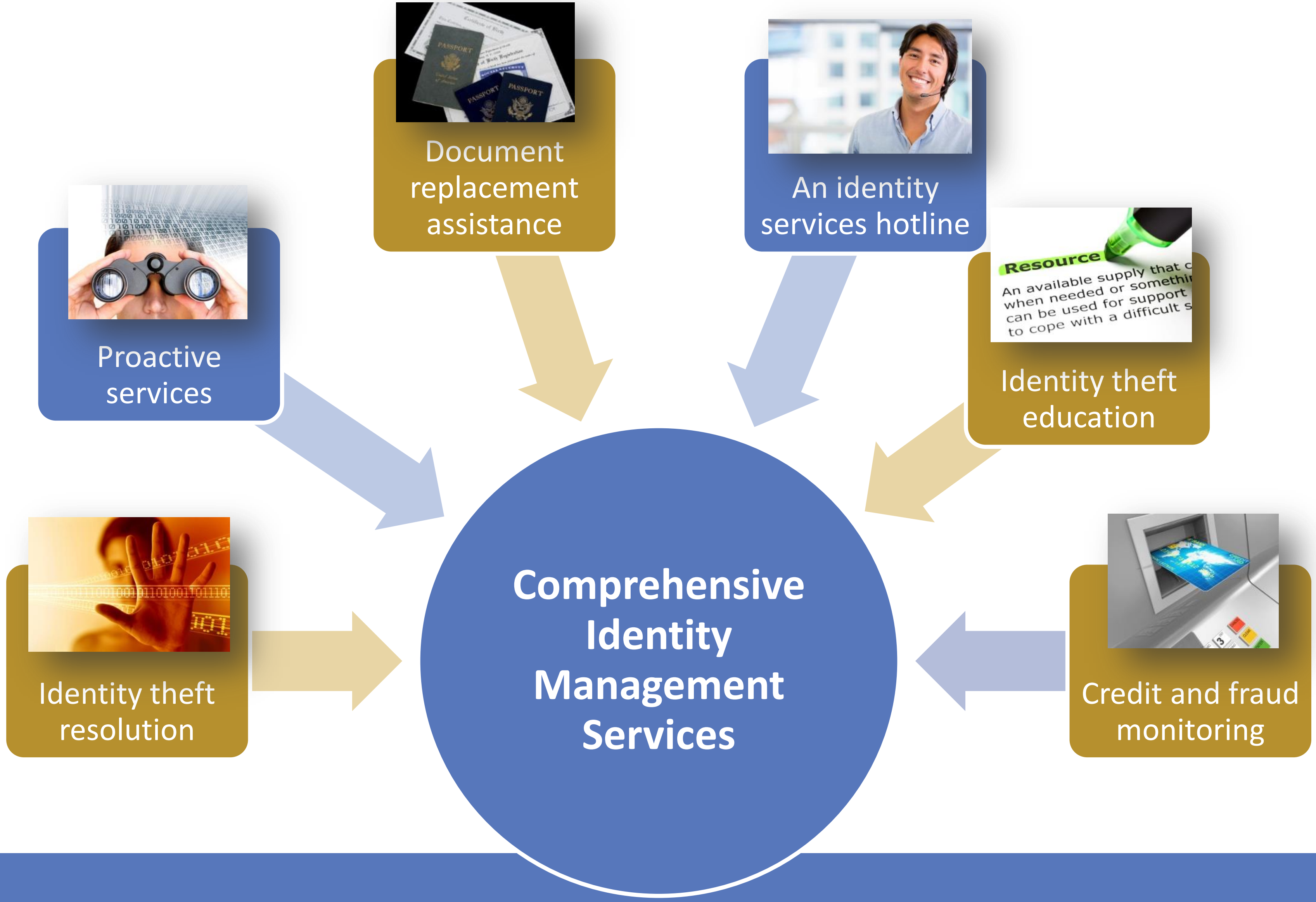
Panic and Uncertainty

Beyond Identity Theft

Who Do They Contact?

Available Solutions

Considering Offering Protection



Document replacement assistance

An identity services hotline

Proactive services

Identity theft education

Identity theft resolution

Credit and fraud monitoring

Comprehensive Identity Management Services

Member Benefits

- **Expert Guidance**
  - Experienced in minimizing impacts and restoring identity
  - Privacy management awareness
  - Guided path for resolving and restoring identity
- **Saves Time and Money**
  - Mitigates potential fraud and out-of-pocket expense
  - Minimizes time to begin resolution and restoration
- **Easy to Use**
  - Full Service
  - Seamless Service
- **Trusted Service**
  - All customers have access to high-touch, one-on-one advocacy from highly trained experts

Benefits to Your Business

IDentityTheft 911
Protecting identities. Enhancing reputations.

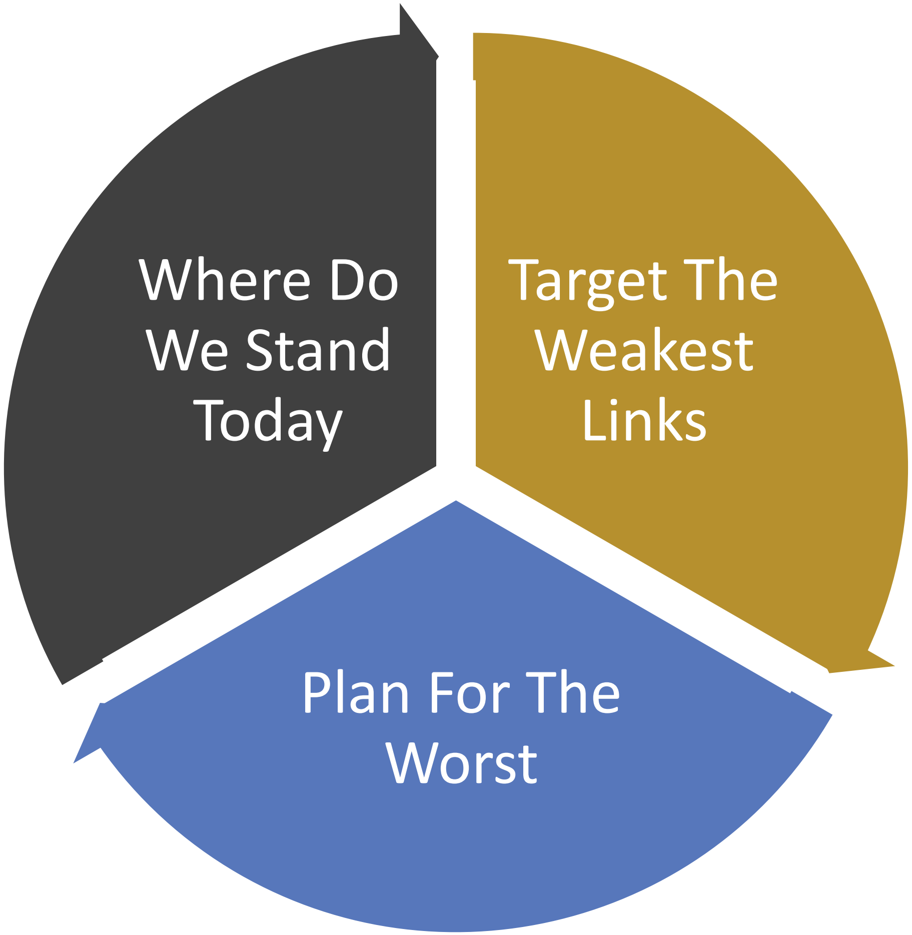
- **Increased Revenue**
  - New & Existing Customers
  - Enhanced Retention
  - Cross-sell Opportunities
  - Risk Free Fee based programs
- **Competitive Edge**
  - Product Differentiator
  - Unique Offering
- **Value-added Benefit for Customers**
  - Proactive & Reactive ID Mgmt
  - Easy to Use
- **Trusted Partner to Handle the Heavy Lifting**
  - Consistent Service
  - Experts to Rely On
  - Seamless Solution
  - Full Transparency

Revenue
Competitive
Trusted Partner
Valued Service

Protecting Your Organization

Your Members Aren’t the Only Ones At Risk

Target Breach Solution

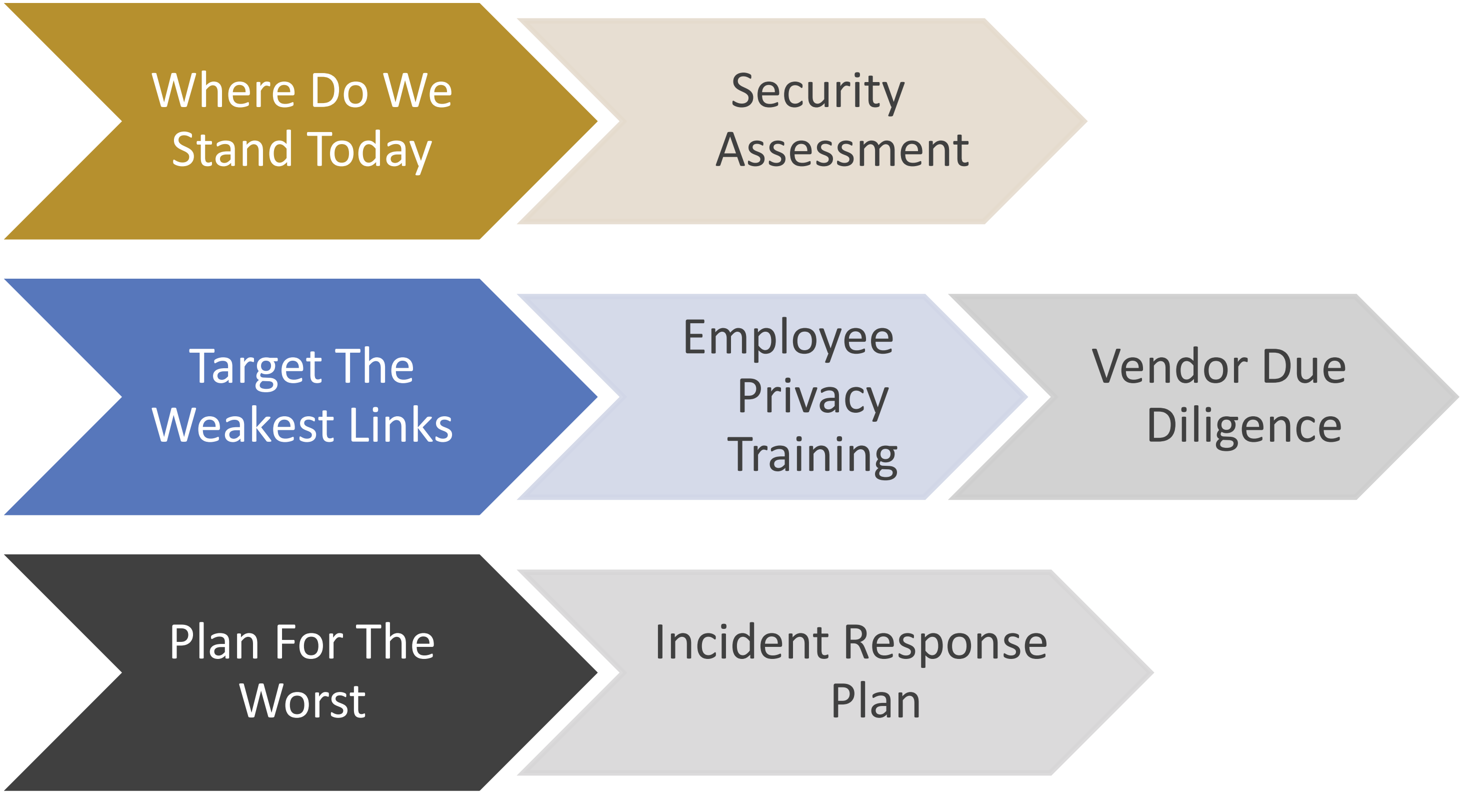


Where Do We Stand Today

Target The Weakest Links

Plan For The Worst

Target Breach Solution



Where Do We Stand Today

Security Assessment

Target The Weakest Links

Employee Privacy Training

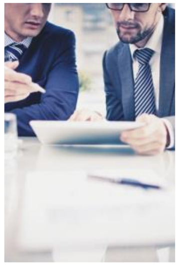
Vendor Due Diligence

Plan For The Worst

Incident Response Plan

Breach Response Areas of Focus

IDentityTheft 911
Protecting identities. Enhancing reputations.



Breach Counseling

Crisis Management

Remediation Planning

Notification Assistance

Evidentiary Support

Why is data security and privacy so important?

Everyone’s Reputation is at stake!

- Turn the growing risk of data breach exposures from a growing expense issue into a member advantage

- Develop multifaceted approach for to empower your employees, members and partners

- Enhance the reputation of your Credit Union by protecting your members’ digital reputation

- **It’s about awareness, recognition, planning, action & response.**

IDentityTheft 911®
Protecting identities. Enhancing reputations.

Thank You

QUESTIONS?

Matt Cullina
IDentity Theft 911
Chief Executive Officer
mcullina@IDT911.com
401.680.4010