MYTHS and MYTH BUSTERS

Myth 1 ▶	My business is too small to be a target for cyber-fraud.
Myth Buster ▶	**NO!** If you are in the title and settlement industry, you are a TARGET.
What to do?! ▶	Thoroughly examine your business to assess the risks present; develop, document and implement policies, procedures, and protections to mitigate those risks and deter fraud.
Myth 2 ▶	Firewalls, Anti-Virus and Anti-Malware software are all the protection I need.
Myth Buster ▶	**NO!** Firewalls, Anti-Virus, Anti-Malware software are absolutely necessary, but it's human error that will allow most cyber-fraud to occur.
What to do?! ▶	Create a culture of fraud awareness. Develop and clearly document processes and procedures. Train and retrain your staff to follow these processes and procedures.
Myth 3 ▶	Once I have been hacked, there is nothing that I can do.
Myth Buster ▶	**NO!** Inaction will only allow things to get worse. Act **F.A.S.T**! The problem will not get better with time.
What to do?! ▶	You need a Cyber-Fraud Response Plan that can be quickly implemented and followed. Time is money!
Myth 4 ▶	Cyber-fraud is only about money.
Myth Buster ▶	**NO!** More times than not, cyber-fraud involves the stealing of information that can be used to steal money. In some cases, cyber-criminals want to destroy information so that your business is disrupted.
What to do?! ▶	Back up your data regularly. Secure the back-up data in accordance with a thorough Business Continuity Plan.
Myth 5 ▶	In the event of a cyber-breach, I should immediately turn off all of my computers.
Myth Buster ▶	**NO!** If you turn off the computers, you may eliminate the opportunity to capture relevant information through forensics.
What to do?! ▶	Disconnect the computer from the internet and network without turning off the computer. Call a forensic computer scientist or law enforcement forensic computer scientist to analyze and review your digital devices and network.
Myth 6 ▶	My E&O insurance will cover me for cyber-fraud.
Myth Buster ▶	**NO!** Generally Professional, General, Liability, and E&O policies have exclusions for cyber-fraud.
What to do?! ▶	Ask your insurance agent about the various types of coverage (coverage for loss of data vs loss of money).

Investors Title
INNOVATIVE BY INSTINCT

121 N. Columbia Street (27514)
PO Drawer 2687 | Chapel Hill, NC 27515-2687
800.326.4842 | **invtitle.com/wire**

B-86 (10/2018)

F.A.S.T.

FAST ACTION STOPS THEFT

Investors Title
INNOVATIVE BY INSTINCT

Damage Control

If you discover a breach or loss of data or money, it will be important for you to understand that the money or data lost is already gone. You will be in "DAMAGE CONTROL" mode. The steps you take will make a big difference in whether you are able to recover any of the money or data lost, and whether you stop additional losses. DELAY and INDECISION are NOT options at this time.

To prepare for the day when (not if), you become a victim of cyber-fraud, you need to have a Cyber-Fraud "Response Plan." You need to know HOW to act **F.A.S.T:** Fast Action Stops Theft! When someone asks you (the bank, law enforcement, or your client) "How long have you known about this?" your answer should indicate a very short time frame, followed by your presentation of documented evidence of all the steps you took when it was discovered. Without a Response Plan, you can do neither.

"There are only two types of companies: those that have been hacked and those that will be." – Robert Mueller, FBI Director 2012

Fast Action Stops Theft!

Avoid Being A Victim – Know Your Cyber-Fraud

Cyber Breach (Loss of Data/Information)

Cyber-Breach Fraud can be perpetrated in many ways including:

- Gaining credentials (login and password) for access to a computer network that contains sensitive information or Non-Public Personal Information (collectively "NPI")
- Intercepting un-encrypted or improperly encrypted communication containing NPI
- Improper disposal of NPI
- Sharing NPI with a source that is believed to be trusted (but is not); and many more

Cyber Theft /Cyber Crime (Loss of Money)

Cyber-Theft Fraud involves gaining wrongful access to a computer and/or a computer network in order to steal or misappropriate money. It can be perpetrated in many ways including:

- Gaining credentials (login and password) for access to a computer network or online banking
- Gaining access to account and routing numbers and withdrawing sums through an Automated Clearing House ("ACH") transaction

Social Engineering Fraud

This fraud is a type of theft that is more dependent upon the traditional elements of fraud and designed to trick an authorized individual into sending money to an incorrect recipient or location. It is characterized by:

- A false representation of a material of fact – whether by words, conduct, false or misleading allegations, or by concealment of what should have been disclosed, with an intent to
  - deceive another
  - coerce an individual to act in reliance upon it, and
  - that, in fact, deceives another to his or her legal injury
- This type of fraud often involves falsified wiring and/or disbursement instructions

Is this Your Old Cyber-Fraud Response Plan?

- Discover breach or loss
- Panic
- Cry
- Call the Bank
- Cry again
- Deny
- Write a big check
- Curse again
- Lose sleep
- Plan to switch careers

If your plan looks similar to the "Plan" above, you are MISSING almost ALL of the ESSENTIAL STEPS that you would need to take if you were a victim of cyber-fraud. You need a well thought-out and documented Response Plan.

"If you fail to plan, you are planning to fail." – Benjamin Franklin

Your **NEW** Cyber-Fraud Response Plan. Consider This.

Plan Essentials

1. Have a Cyber-Fraud Response Team
2. Have a Cyber-Fraud Response Plan
3. Act **F.A.S.T** when Cyber-Fraud is Discovered
4. Follow Your Response Plan
5. Review and Update Your Response Plan

DO NOT PANIC. Execute your Response Plan. Follow the Steps to Your Plan in Order.

New Response Plan

1. **Alert the Response Team**
2. **Alert all internal employees**
3. **Take all Computers OFFLINE;** Do NOT turn them off unless and until directed by your IT professionals
4. **Immediately Contact your Bank(s)** (team member with the responsibility should have the proper account(s) authorization(s) to discuss and direct activities with the bank)
   - For **ALL CYBER-FRAUD** incidents (not just financial losses):
     - Contact your bank's central fraud department (in addition to local branch)
     - Monitor all of your accounts for any improper activity
   - When **MONEY IS LOST** or misdirected:
     - Immediately attempt to stop or recall any improper outgoing wires/checks/transfers
     - Use the word "Fraud" in your communications with the bank(s)
     - Direct sending bank's fraud department to issue a ***Letter of Investigation (LOI)*** from sending bank to receiving bank providing details about the fraud and directing them to hold the money.
     - If wire is over $50,000, direct sending bank to initiate **FBI's Financial Kill Chain**
     - If an international wire, direct sending bank to issue **SWIFT** recall notice
     - Contact receiving bank yourself and request that funds be frozen
     - Continue to regularly follow up with both sending and receiving banks to make sure they follow through
5. **Contact FBI**
   - File a report with the FBI Internet Crime Complaint Center at www.IC3.gov (see Response Plan Documentation form)
   - Contact local FBI field office (https://www.fbi.gov/contact-us/field-offices)
6. **Secure Your Office and Your Network**
   - Change/Update all passwords with new strong complex passwords
   - Secure the physical premises
   - Preserve evidence; do NOT delete or move emails
7. **Document the specifics of the breach and/or loss;** see Response Plan Documentation form
8. **Contact your Cyber-Fraud Insurance Carrier(s);** if you have one; follow their additional instructions to make sure that your coverage remains intact
9. **Contact Your Errors and Omissions and other insurance Carrier(s);** follow their additional instructions to make sure that your coverage remains intact
10. **Contact Law Enforcement/Local and State Authorities** (Police, Sheriff, SBI, etc.)
11. **Contact State Bar and/or other regulatory authorities that govern your activities**
12. **Contact Title Insurance Underwriters** (if breach involved a real estate transaction)
13. **Follow Laws Regarding Notification of Your Clients** (if necessary and/or advisable)
14. **Review and Update your Response Plan**
    - Assess Firm / Company Priorities regarding resources and risk associated with breach/loss
    - Determine if breach or loss could have been prevented by different policies and procedures
    - Adapt Firm / Company processes and procedures to ensure that a breach/loss will not happen again

Cyber-Fraud Response Team

1. No business is too small to have an internal Cyber-Fraud Response "Team" responding to a cyber-fraud breach.
2. Your Cyber-Fraud "Response Team," no matter the size, will be responsible for quickly taking all of the steps necessary to reduce your losses (data or financial), possibly increasing your chances of recovery and decreasing the chances of suffering additional losses.
3. Appointing more than one person to execute your Cyber-Fraud "Response Plan" allows for multiple steps to be executed at once.
4. Assigning each Response Team Member the responsibility of executing one or more tasks in the Response Plan will ensure that everyone knows what to do.
5. Your Response Team should include an expert in Cyber Security and IT matters (may be internal or external). Do not wait until you suffer a breach to identify and establish this relationship.