TRISTATE CAPITAL

Fraud Alert:
A Social Engineering Survival Guide

www.TriStateCapitalBank.com

It happens so quickly, and apparently so innocently – and family office and wealth management personnel, who may not have the extensive training and resources to fight financial fraud, seem especially vulnerable.

The phone rings, and it's a new client's executive assistant asking about an updated balance on the account, and checking on a recent transaction.

The call seems innocent enough. After all, clients call asking for information on their accounts all the time. Most importantly, the assistant was able to verify all the account information.

One week later, the assistant calls back, asking you to wire funds to a third party account. All the critical data – account numbers, Social Security number and recent transaction activity is confirmed. That day, the wire transfer is completed.

The next day the client calls - all the money in the account has disappeared, and the client angrily demands an explanation. That's when the reality hits home – your Family Office has been targeted and tapped into by a financial fraud artist – and there is no way around total and complete responsibility for the loss.

social engineering - the term security experts use to describe fraud campaigns that target human, and not technology elements

If you think that your security system and fraud training is sophisticated enough to keep scam artists at bay, think again. Social engineering scams are growing in size, occurring with increased frequency, and are becoming more threatening.

Consider that financial fraud attempts reached all-time record highs, rising by approximately 4,000 percent since 2010, according to the 2012 Data Breach Investigations Report.

Now social engineering – the term security experts use to describe fraud campaigns that target human, and not technology elements – has grown increasingly more pervasive.

In fact, with technology-based security programs becoming more sophisticated, closing gaps that criminals used to use to gain access to confidential data, social engineering fraud is growing. This type of fraud has become the de facto doorway for criminals to uncover personal data such as phone numbers, addresses, mothers' maiden names, pets' names and hobbies from online public databases and social media sites, and use that information to manipulate employees into giving away confidential information.

Studies show that 97 percent of social engineering breaches are avoidable, as fraudsters select staffers, managers, and other personnel because they are deemed "easy" targets.

Meanwhile, as firewalls and software solutions grow in sophistication, financial fraudsters are keeping up by varying their tactics. This means that social engineering specialists have the ability to bypass automated security systems and focus directly on unsuspecting executives and staffers who unknowingly pass along critical corporate data, setting the stage for fraud.

In this white paper, Fraud Alert: A Social Engineering Survival Guide, TriState Capital walks you through some of the social engineering landscape, suggesting ways in which your company may be at risk and what you can do to prepare for and reduce it at your firm.

Inside this report, you'll learn . . .

- The ABCs of social engineering.
- The mindset of social engineering scam artists.
- Why managers and staff members are susceptible to social engineering scams.
- Ways to train employees to recognize social engineering scams – before the trap is set.
- Specific tools your company can use to thwart social engineering.

What Is Social Engineering?

Social engineering describes a data breach attempt that leverages human interaction to manipulate employees to deliver personal financial data that financial con artists can use to defraud clients of their money. It is not a technology-based fraud campaign.

The phrase "social engineering" is broadly defined as an attempt to gain access to information, primarily through manipulation and misrepresentation. Social engineers are fraud artists that try to take advantage of the trusting nature of many customer service employees. They need direct contact with these staff members to extract critical client data.

For instance, a scam artist trying to breach a computer network may attempt to gain the trust of one of your staff members and lure them into revealing critical data that compromises the network's security. Social engineers typically rely on the trusting nature of employees – and they rely on their tendency to want to help to the point of opening up and offering too much information. They may, for example, contact the staffer with an urgent problem that requires immediate network access. The con artist may use several tactics to extract that information, including an appeal to vanity, an appeal to authority and the fact that the employee may have his or her guard down in the face of an imminent "crisis".

You Are the Weakest Link

- Social engineering is commonly used to gain sensitive information.
- Don't give out even "trivial" information.
- Social engineers rely on human nature to commit financial fraud.

Step 1

Before You Can Actualize, You Must Recognize

So what can wealth management executives and staff members do to stop a social engineering attack like the one mentioned above in its tracks?

Step #1 is the most important step, because to recognize an attack is to begin to prevent it. Be aware of how financial scam artists can use public information, like Social Security and investment account numbers, to wreak havoc on customers – and on your business.

When executives and staff members understand that technology is not the be-all and end-all solution to financial fraud, you'll be a step ahead. That's because virtually all financial services firms, including wealth management firms, have security firewalls and other security measures in place. However, social engineers recognize that the real risk/reward comes from targeting people – not computers.

Use that knowledge against financial fraudsters by taking these concrete steps:

Get a grip on your client information
As a family office executive, it's imperative to take the reins and control the flow and access of critical client data within your company.

By and large, the less information that is given out to staff members, the better. Install access controls in your company's software database to control who can obtain client data and who can't. Think of it this way – the fewer people with access to client data, the harder it is for social engineers to leverage employee access to information and use it to commit financial fraud.

Build a social engineering "security squad"
Even if you have limited resources, it's a good idea to have one or two trusted "first responders" in line to create and enforce a documented protocol to detect, report and respond to attempted financial fraud events. "Job One" is for employees to have a direct line to a security team when social engineers strike.

> "Job One" is for employees to have a direct line to a security team when social engineers strike.

Build skepticism in your workplace
Most wealth management firms don't seek to build a culture of distrust in the workplace, but given the severe threat from social engineers, healthy skepticism is needed. The key is to emphasize diplomacy, especially when staff members are interacting with clients, their family members and employees via e-mail or over the phone. Family office employees should always be polite and helpful, but any sense that a call for information is out of place should be acted on promptly. When such a contact situation arises, have your staff members respond to a suspicious call or e-mail by answering "Let me take your contact information and we'll get right back to you." Then the employee should report the incident straightaway to the first-response team.

Peel the mask off of impersonators
Recognition is the key to thwarting social engineers. A favorite tactic of fraud artists is to pose as an insider who can credibly pass themselves off as someone in your organization, or someone outside your company who seems legitimate and poses no security risk – even as they pry critical client data loose. Usually, "impersonators" present themselves through traditional communications channels, like by phone, e-mail, or even in person. Staff members and managers need to resist the high-pressure efforts from fraudsters to release information such as Social Security Numbers or client account passwords. With good, solid social engineering guidelines in place, employees can feel secure turning down all requests for sensitive client information that aren't strictly legitimate.

Three Key Recognition Points

1 | Most social engineering is performed via phone.

2 | Attackers will typically call an employee masquerading as a trusted source (such as the executive assistant of a high-level client, or an information technology staffer or a contract employee).

3 | What's the risk? The information given out to social engineers may be considered, at first glance, inconsequential. But fraudsters use even the most banal piece of information as a "next step" to building more information. Even the mention of a client's name is a valuable slice of data for a social engineer.

Step 2

Training Game: How To Prevent Social Engineering Scams

There's no doubt that family offices focus on the "personal element".

After all, wealth management practices place a high priority in customer service, and usually, the more interactions between the "human element" (i.e., staffers and clients), the better.

But social engineering scammers have broken the code, and have figured out how to leverage that person-to-person interaction and successfully use customer data to commit financial fraud. In fact, some techniques are so effective they're used time and time again.

Consider this pervasive social engineering scam:

- Using the IT administrator's name, an attacker will pose as the IT administrator or someone working for the IT administrator.
- That fraudster will then inform the employee that IT noticed a problem with the user's computer.
- They will ask the user to perform several functions to gather information, like the computer's IP address.

The attacker will then tell the user that an application needs to be executed on his computer to fix the problem. But that application is actually a sophisticated piece of software designed to gather the private personal data and account information of your clients. Once collected, that information will be used to perpetrate financial fraud against your clients.

The key to stopping most scams like this one is simple - and highly effective:

Wealth management firms should implement a consumer awareness program, train staff members about potential social engineering scams and should educate those staff members on the very specific customer data points never to share with outsiders.

For example, any combination of components of customer information that would allow someone to log on to or access the customer's account, such as username and password or password and account number should never be shared with non-approved individuals.

Watch For "Nibblers"

So-called nibblers may attempt to build their fraud campaign on a piece-by-piece basis:

- Social engineers often contact several different employees to gain information.
- Separate pieces of information provided could seem trivial to each employee.
- If pieced together, all the information could lead to a security breach.

Make sure to train staffers on social engineers who may initiate multiple contacts targeted at multiple employees. Any suspicious e-mail or phone call should be brought to the attention of management – once the contact information is made available to all staffers, the chances of a "nibbling" data breach are greatly reduced.

Step 3

Play Defense Against Attacks Via Multi-Factor Solutions

Family office practitioners must recognize multi-factor attacks, especially the ways in which scammers attempt to build a detailed portrait of their intended victims by using e-mail, phone transfers and other media to gather information.

Even the most innocuous query from a seemingly legitimate source can breach a company's strongest firewall.

Thus, there is a need for a multi-layered social engineering defense that includes several critical ingredients, all of which come in large part from the Federal Financial Institutions Examination Council:

"Something you know" – Employees dealing with the public must obtain concrete personal client data before releasing any information. Ideally, that includes a password, a PIN number, or personally identifiable information (PII).

"Something you have" – In cases involving especially sensitive data in face-to-face interactions, employees should always ask for personal identification (ID), bank debit card, phone number or security token.

"Something you are" – Usually biometrics, like retina scanning and fingerprinting can stop a social engineer cold.

A combination of any two of the multi-level defenses listed above, along with some clear, compelling and concise security guidelines can help prevent social engineering-driven financial fraud.

For example, if a call comes into the office, employees should never rely on what the caller says he or she knows, but should validate the caller by the "something you know" and "something you have" client information firewalls.

Always use physical security and digital authentication safeguards that require multi-factor authentication – two or even three layers are usually sufficient – before granting access to client data. If especially sensitive asset is being requested, always ask for multi-factor authentication using more than one employee. Double-checking such data with another staffer or "up the chain" from a manager is a highly reliable safeguard against social engineers.

Deploying multi-layered defenses against financial fraud artists enables wealth management firm employees to authenticate clients without sacrificing high-level customer service, and without being victimized by social engineers. Ultimately, it's all about securing your data network without compromising quality customer service. Preventing social engineering fraud is a balancing act – specifically, balancing customer service and skepticism.

Keys To Stopping Social Engineers

1 | Never give out your clients' personal financial information in response to an unsolicited phone call, fax, or e-mail – no matter how official it may seem.

2 | Do not respond to e-mail that may warn of dire consequences to a client unless information is validated immediately. Contact the company to confirm the e-mail's validity using a telephone number or Web address you know to be genuine.

3 | Urge your clients to check their credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Discrepancies should be reported immediately as information obtained via these small thefts can be used to create a social engineering profile and perpetrate a scam.

4 | Suggest that your clients set up a fraud monitoring service. Some of the services offered include frequent credit score checks, public record surveillance, and enhanced checking and savings account application alerts for certain transactions.

Step 4

Weigh the Risk – Then Act

As a family office executive, you know how important it is that your team doesn't alienate clients by being too cautious around transfer and withdraw requests. On the other hand, it's even more important to avoid becoming the victim of a scam.

That balancing act is all about managing risk. And that means the proper management of all your firm's client data.

Wealth management executives should begin this process by inventorying all relevant applications and determining the level of risk for each one.

- Items to be considered as part of this process include the customer type, transactional capabilities of the application, sensitivity of information displayed or imputed, ease of use and volume of use. Current controls for authentication should also be noted.

- Sign up protocols for new clients should be recalibrated as well. For new customers opening an account via an application, analyze controls and confirm appropriateness. If new customers are permitted to open new accounts online, stringent controls should be in place to confirm identity. These should include positive verification (i.e., comparing information to a credit report), logical verification (e.g., do the telephone area code, zip and street address match) and negative verification (e.g., an Office of Foreign Assets Control of the U.S. Department of the Treasury check).

- Effective monitoring and reporting should be established as a detective control. High-risk applications should have sound reporting mechanisms that alert security administrators when there is evidence of suspicious activity. A monitoring and response function should receive and respond to incidents in a timely fashion.

Once the Risk Assessment has been completed, any high-risk application should be identified and multifactor authentication, as described above, should be implemented. There is no one solution or list of solutions that is required, and the solution should be appropriate given the nature of the application.

Sample Social Engineering Email

Social engineers often use email to breach data security. Staffers need to confirm the legitimacy of any email request for money with management – even if that request ostensibly comes from the top of the corporate food chain.

FROM: Your Client
TO: Your Staffer
DATE: June 1, 9:50 AM
SUBJECT: Money Missing – Send Cash

Hi (name). While on that business trip to Munich I was robbed and all my cash was stolen. I need you to wire me $10,000 via Western Union.

Here is the WU link: http//www.westernunion.com5643vj

Thanks for your help – please send money ASAP.

Several keys to handling a suspected social engineering email request for money:

- Did you initiate the contact? Invariably, email scams are launched without the request of the staffer.

- Do you recognize the sender's email address? Does the sender normally communicate via email? If not, the chances of a social engineering scam are high.

- Did your staffer get an email that he or she would not typically receive during regular business hours? Typically, email requests for money that come after business hours are a big red flag

Step 5

Learn To Walk That "Fine Line"

There is a fine line between customer service and skepticism. Sure, every family office executive wants to put customer satisfaction above all else, but when should you be skeptical? Communications between a staffer and any client, let alone any individual, should never use an entire account number, for example.

One proven tactic is to limit the information staffers have on hand. Wealth management executives should reduce the amount of personal information in client communications.

After all, social engineering thrives on information, so the less unnecessary personal information disclosed the better.

In addition, family office practitioners can further that "fine line" by . . .

Creating a culture that highlights information security awareness. Employees should be educated and fully cognizant of potential social engineering threats.

Always Verify

In the end, the best strategy in fighting social engineering fraud can be summed up in one word – verify.

In addition, firewalls against social engineers should be formally embedded into the company culture, and fully supported by a training program that is regularly fine-tuned and tested by management, and that offers "buy-in" from front-line employees.

Be Vigilant, Be Prepared and Be Proactive

With a properly trained workforce that recognizes social engineering tactics and knows how to take the necessary steps to handle sensitive data requests, keeping social engineers at arm's length is highly doable.

It's up to you, the wealth management executive, to make sure your staff has the tools and strategies needed to stop social engineering campaigns before they take root and defraud your clients and your company.

In that regard, fighting social engineering fraud is no luxury.

It's a necessity.