How to detect an identity thief

Identity theft may be one of the oldest techniques in the fraud book, but it remains prevalent, especially in a world where much more information is shared than in the past. In 2017, the number of identity theft victims in the U.S. reached 16.7 million—an 8% increase from the previous year.[1]

Contrary to what some may believe, not all fraudsters are geniuses who can outsmart advanced technology. Some are more unassuming but know how to take advantage of people's natural inclination to trust others. Meanwhile, these criminals are getting more sophisticated in their attacks by using stealthier, more complex schemes.

Recently, Schwab has seen an uptick in impersonation calls, with fraudsters becoming more sophisticated in their attempts to gain access to client accounts through social engineering. Social engineering is the use of deception to manipulate others into divulging personal information or transacting on a client account. Typically, an unauthorized individual assumes the identity of a client or tricks another person into believing they are a trustworthy source.

We're noticing that criminals are leveraging stolen client information gathered from other companies' breaches, purchased from the dark web, or gleaned from social media to pose as clients. Impersonators use these details—in combination with other tactics—to appear more legitimate. For example, they may spoof the client's phone number or use a voice changer to sound like the client. These imposters often are calling to update account information such as email address, password, or phone number, or to initiate or approve money movements.

Social engineering is swiftly becoming a universal threat—one that can have big impacts. It is a clever, often misunderstood, and overlooked form of identity theft because, while it still requires a certain amount of finesse and skill, it doesn't require the technical expertise necessary to hack into a major bank's computer network and reroute funds.

Social engineering may occur via phone, email, or social media. Often, the scammer will use skills such as charm, friendliness, wit, or urgency to build a sense of trust with the victim. This is intended to convince the victim to either release unauthorized information or perform actions that benefit the scammer, such as sending money. It is also very common for the scammer to visit social media sites to obtain identifying information to bolster their credibility.

Fraudsters will sometimes rely on human error to obtain additional information. For example, while answering a security question about previous employers, they may rely on a LinkedIn profile. If their first answer is incorrect, the fraudster will guess again and dismiss the incorrect answer by quickly saying something like, "Oh, I only worked there for three months, so I didn't think that was the correct answer." Despite receiving an incorrect answer initially, a customer service representative might not press further or ask additional security questions.

Fraudsters will also try empathy, such as pleading, "My daughter, Susan, was celebrating her birthday at the park today and is seriously injured. I'm calling from the doctor's office, and they are requiring that I pay cash before she can be seen. It's urgent that I access my account right now, but I locked myself out. Can you please help?"

Additionally, they may employ distraction techniques, such as a crying baby or other background noises, and ask the professional to repeat questions, claiming that they cannot hear or that there's a poor connection. Usually, they're hoping that the customer service representative gets frustrated or loses concentration.

8 tips to prevent identity theft
Knowledge and awareness can help you protect your firm and clients against cybercrimes such as identity theft or social engineering. Here are some best practices:

1. Safeguard your firm's information and your clients' personal data.
2. Limit whom you trust with your and your clients' personal information.
3. Use caution when sharing information and personal details on social media.
4. Consider how you interact with clients via email or phone, and be selective about disclosing details.
5. Be aware of your surroundings when talking on the phone. Do not hold conversations regarding your role or client interactions in public places.
6. Look for transactions that are outside of your clients' normal patterns of behavior.
7. Employ strict authentication protocols that you follow for every transaction—no exceptions. For example, you may choose to video conference with your clients or require a verbal password or security questions for accounts.
8. Educate and train your staff to ensure they are talking to your true client.

7 red flags to identify imposters
Several things will help you identify a possible imposter:

1. Atypical background noises, e.g., a crying baby or loud traffic, to distract the representative and expedite the call.
2. Age and gender appropriateness of the voice: If the client is 85, does the caller's voice match that age?
3. Frequent pauses when asked a simple verification question.
4. A robotic-sounding voice, which indicates the caller is using a voice modulator to disguise their real voice.
5. Asking you to repeat simple questions, e.g., "Did you ask me for my mother's maiden name?"
6. The sound of paper being shuffled in the background.
7. A call from a number that is not on record.

What is identity theft and how does it happen?
Identity theft occurs when one person uses another person's identifying information to assume their identity for the purpose of committing fraud or other crimes.

This type of fraud can be executed in person, verbally, or electronically, and can be familial (attempted by a family member) or external (attempted by an unknown party).

Electronic channels are the most common paths for identity theft, and fraudsters can use several different methods to steal a victim's credentials, such as phishing or malware.

Identity theft falls into two categories:

1. Low-tech methods: These may include posing as a trusted person for the purpose of financial gain or to access information. For example, the identity thief may contact a call center or call you directly, posing as the client.

Other low-tech approaches include taking physical possession of devices, ATM cards, financial statements, and other materials that contain the client's information.

2. High-tech methods: Once identity thieves have the information they need, they may log in to a client's account to gain additional data, intercept verification codes, redirect devices, initiate withdrawals, change account details, and more.

Identity theft is a broad topic, so these examples are not all-inclusive and may overlap with other methods that also result in a loss of client information.