



Fraud Encyclopedia

Updated June 2018

Contents

Introduction	3
How to use this <i>Fraud Encyclopedia</i>	3
Email account takeover	4
1. Emotion	7
2. Unavailability	7
3. Fee inquiries	8
4. Attachments	9
5. International wires	10
6. Language cues	10
7. Business email compromise	11
Client impersonation and identity theft	12
1. Social engineering	14
2. Shoulder surfing	14
3. Spoofing	15
4. Call forwarding and porting	16
5. New account fraud	16
Identical or first-party disbursements	17
1. MoneyLink fraud	19
2. Wire fraud	19
3. Check fraud	20
4. Transfer of account (TOA) fraud	20
Phishing	21
1. Spear phishing	23
2. Whaling	24
3. Clone phishing	24
4. Social media phishing	25

Scams	26
1. Properties	28
2. Romance/marriage/sweetheart/catfishing	28
3. Investments/goods/services	29
4. Prizes/lotteries	29
5. IRS	30
6. Payments	30
Other cybercrime techniques	31
1. Malware	33
2. Wi-Fi connection interception	34
3. Data breaches	35
4. Credential replay incident (CRI)	37
5. Account online compromise/takeover	37
6. Distributed denial of service (DDoS) attack	38
Your fraud checklist	39
Email scrutiny	39
Verbally confirming client requests	40
Safe cyber practices	41
What to do if fraud is suspected	42
Schwab Advisor Center® alerts	43

Introduction

With advances in technology, we are more interconnected than ever. But we're also more vulnerable. Criminals can exploit the connectivity of our world and use it to their advantage—acting anonymously to perpetrate fraud in a variety of ways.

Knowledge and awareness can help you protect your firm and clients and guard against cybercrime. When you know how to identify the most common threats and schemes that cybercriminals and fraudsters use to access clients' information and assets, you can help prevent attacks. Use this guide to learn some common cybercrime trends within the financial industry.

The arsenal of tools that cybercriminals use is expansive. And attacks often involve a variety of tactics used in conjunction with one another, making each scenario complex and unique. While this guide is not meant to be inclusive of all fraud techniques, it gives you a place to start.

Never let down your guard

Keep in mind that fraud may not occur immediately after an individual's information is compromised. For example, the intent of a data breach might be to harvest personal information to sell on the dark market. This information, in turn, may be used by other cybercriminals to commit a fraudulent act later. Or malware may be installed on a device but not activated until months later. Another common scenario is a compromised email account that is left untouched while the fraudster monitors the account in the background waiting for the right moment to request a wire.

Schwab's online resources

To learn more, we encourage you to visit our [Cybersecurity Resource Center](#) where you can find a wealth of tools, education and resources to help you build and strengthen your cybersecurity plan and detect and prevent fraud.

Always be on the defense, and remember that fraud can occur at any time.

How to use this Fraud Encyclopedia



You are welcome to use this resource however it best fits your needs. Here are some suggestions:

- Print the PDF version and have employees read it cover-to-cover, including incorporating it into an employee onboarding process
- Provide it to staff to supplement training
- Use the online version to take advantage of the links throughout the document
- Reference it on an as-needed basis to refresh your knowledge

At the end of this document you'll see a fraud checklist divided into several sections. You may wish to print this information and keep it handy as a reminder. The checklist may be used as a starting point that you customize to align with your own policies and procedures. We've also provided a list of current Schwab Advisor Center® alerts, so you know which alerts are available.

Because the world of cybercrime is constantly changing, we anticipate that this document will be updated on an ongoing basis. Please check back periodically and refer to the date on the cover to confirm you are accessing the most recent version of this document.

If you have questions or feedback, please contact your Relationship Manager or your service team.

Email account takeover

What is it?

Cyber thieves gain unauthorized access to an email account—often through the theft of online credentials, **phishing**, and **social engineering**—to perform acts such as:

- Searching for sensitive, non-public, personal information such as Social Security numbers, income, and account balances, with the intent of committing fraud
- Finding emails containing log-on credentials (e.g., user names and passwords) to use or sell the information
- Posing as the client by inserting themselves into the email conversation and requesting unauthorized transactions
- Using the “Forgot User Name” or “Forgot Password” functionality on a site to gain access to accounts and update the account holder information prior to initiating fraudulent transactions
- Taking control of the account and denying access to the legitimate email account owner
- Monitoring email traffic over a period of time by routing new emails to an alternate folder (i.e., deleted folder) and then manually moving them to the inbox after they’ve been reviewed


At Schwab, we typically see the criminal posing as the client and engaging in electronic communication with the client’s financial advisor to facilitate disbursements.

How does it happen?

Fraudsters gain access to an email account using different methods, such as:

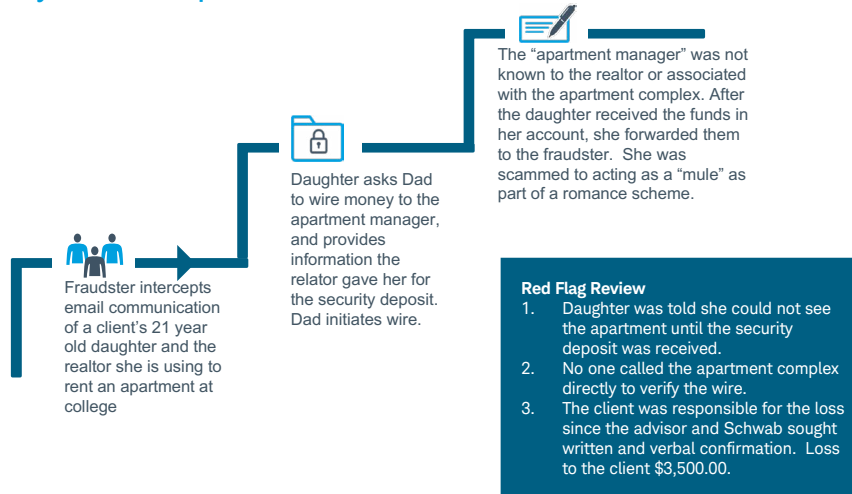
- Obtaining stolen credentials
- Spoofing the client’s true email address by using an email address that is very similar (client**1234**@anymail.com vs. client**1234**@anymail.com)
- Changing the email address on an account to one that is controlled by the fraudster

Resources

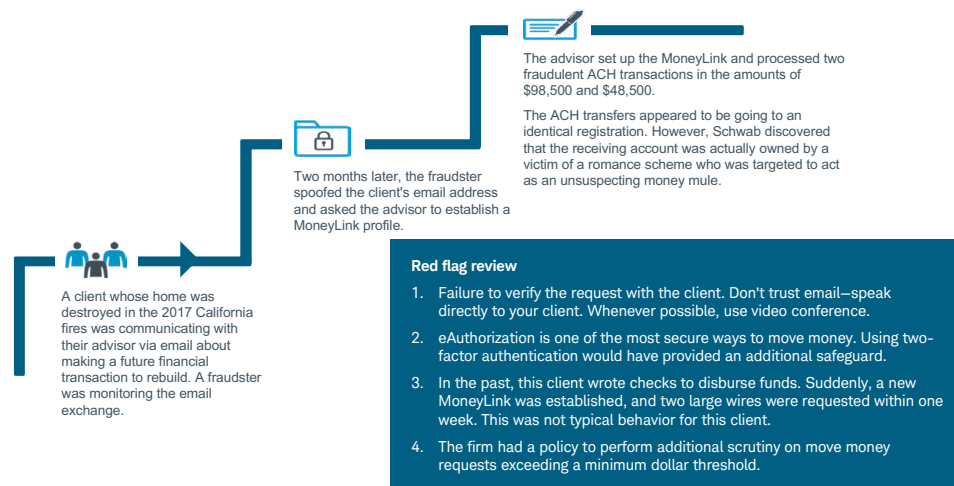
- Schwab’s Cybersecurity Resource Center 
- U.S. Department of the Treasury FinCen Advisory
- Two Factor Auth

Case study examples

Case study: A new apartment



Case study: California fire victim and money mule victim



To prevent email fraud, you should always apply additional scrutiny when engaging in email correspondence and never rely on email to initiate money movement requests.

Tips for you and your firm:

- Require that clients use Schwab's Electronic Approvals tools.
- Verbally confirm disbursements, using video chat whenever possible.
- Apply authentication methods that are detailed and customized to your business, such as using a unique passphrase that only you and the client know.
- Do not use email to disclose details and personal information that can be used by the fraudster.

Tips for your clients:

- Encourage your clients to follow secure email and cyber practices. This can include using strong, unique passwords for all sites and/or two-factor authentication when available.
- Run regular virus scans.

Keep reading for more information on specific types of [email account takeover](#) »

1. Emotion

What is it?

Fraudsters may employ sympathy, aggression/threats, or urgency to manipulate advisors into bypassing procedural protocols.

How does it happen?

Fraudsters will present false pretenses for the funds disbursement or express emotions that may persuade an advisor to make special accommodations to appease the “client,” such as expediting the request or not requiring verbal client confirmation.

Example(s)

- “I need the funds for my nephew’s funeral.”
- “I am very ill and need the money for medical expenses.”
- “Funds are critical for a pending property closing.”
- “Money is needed for wedding expenses.”
- “This is for a <family, medical, financial> emergency.”
- “I need immediate assistance, or I’ll consider taking my accounts elsewhere.”

Tips to prevent or identify

- Don’t be fooled by appeals to your emotions to skirt your security protocols.
- Remind your clients that your established verification processes help you both work together to protect their accounts. Providing transparency can help your clients understand the reasons for the requirements and better set expectations.

2. Unavailability

What is it?

To circumvent standard validation processes, fraudsters often indicate they are unavailable in person or by phone.

How does it happen?

Criminals will create scenarios that help give the impression that a verbal verification is logistically impossible. Advisors are then manipulated into relying on email communication to conduct business.

Example(s)

Typical scenarios include:

- Meetings
- Traveling/out of the country
- No reception
- Physical inability to speak (laryngitis or other medical issues)

Tips to prevent or identify

- Stay firm on authentication procedures.
- Offer alternatives such as in-person or video conferencing.
- Remind your clients that your verification processes are critical to secure their account safety.

3. Fee inquiries

What is it?

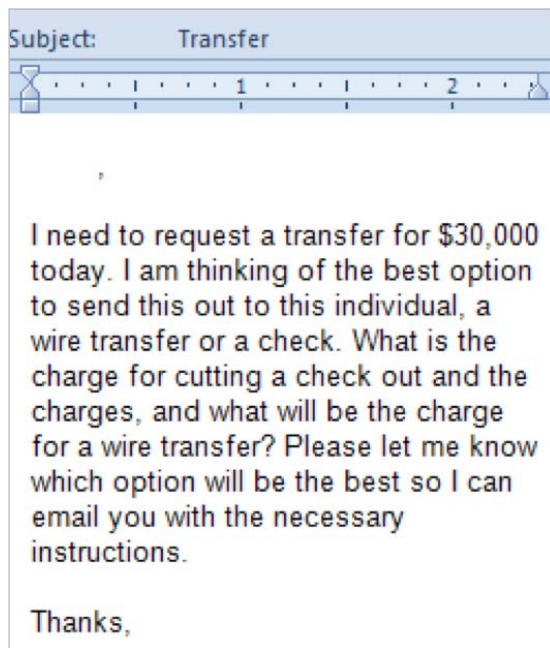
This form of fraud often includes inquiries about the difference in fees for various disbursement channels.

How does it happen?

Criminals will often inquire about the difference in fees between an overnight check and a wire. At Schwab, there have been several instances in which the criminal has sent the same email to multiple advisors, hoping that at least some will be distracted and think the email is genuine.

Example(s)

Below is an example of a common email template sent to financial advisors. This verbiage has been sent to advisors dozens of times to attempt to enact fraudulent checks or wires. Often these requests are for even-dollar amounts between \$20,000 and \$40,000 and result in overnight checks to third-party individuals.



Tips to prevent or identify

- Verbally verifying transactions with your clients is the best defense against these types of fraudulent requests.
- If you receive an email that resembles this template, escalate it internally within your firm and notify your Schwab service team.

4. Attachments

What is it?

Emails may include attachments such as invoices, receipts, subscription documents, or other items that give the payment or disbursement request a false appearance of legitimacy.

How does it happen?

Fraudsters may present extra details or provide documents within the email that make the disbursement more credible. This helps in deceiving advisors into accepting the request as legitimate and distracts the recipient from the true intention of the funds.

Example(s)

These documents have been sent to advisors on multiple occasions.

Tips to prevent or identify

- Do not allow details and supporting documentation to convince you that the distribution request is reasonable and legitimate.
- Continue to follow your policies and procedures as you would for any disbursement request.

Subscription document:

Investor/Member No.: _____

SUBSCRIPTION AGREEMENT
of
ABC TRADING CO LTD
A Hong Kong limited liability company

The undersigned purchaser ("Purchaser") hereby subscribes to become a Member in ABC TRADING CO LTD (the "Fund") and to purchase a Membership Interest in the Fund by investing the amount indicated below, all in accordance with the terms and conditions of this Subscription Agreement, the Amended and Restated Limited Liability Company Operating Agreement (including any amendments thereto) (the "Operating Agreement"), and the Private Placement Memorandum of the Fund (including any amendments thereto) dated February 1, 2016 (the "Memorandum"). All capitalized terms used herein, but not defined herein, shall have the meanings ascribed to them in the Memorandum.

1. SUBSCRIPTION FOR MEMBERSHIP INTERESTS

AMOUNT OF INVESTMENT: \$ 421,374.23

EXACT NAME OF PURCHASER(S): Dollar and Penny Partners, Inc.

FORM OF OWNERSHIP: Please indicate the form of ownership in which Purchaser will hold title to the Membership Interest. Purchaser should seek the advice of an attorney in deciding because different forms of ownership can have varying gift tax, estate tax, income tax and other consequences. Check one:

INDIVIDUAL OWNERSHIP
 COMMUNITY PROPERTY with right of survivorship
 JOINT TENANTS WITH RIGHT OF SURVIVORSHIP
 TENANTS IN COMMON
 GENERAL PARTNERSHIP
 LIMITED PARTNERSHIP
 CORPORATION
 LIMITED LIABILITY COMPANY
 TRUST
 IRA OR KEOGH PLAN
 PENSION, PROFIT SHARING PLAN OR RETIREMENT TRUST

PURCHASER(S)' *BESS Main, Stone, Goldover, San Francisco, CA 94108*

Invoice for a work of art:

WAN WAN BLDG
14-24 MAWAH CHOI S ST
MK, HONG KONG.
DIME AND QUARTER INTERNATIONAL LIMITED

Nancy Nickel
755 Silver Dollar Way
Paradise Valley AZ, 85494
United States of America

Invoice #10 HK1111-GZ123
January 2017

INVOICE

Edward Willis Redfield
"Cherry Blossoms Above the Delaware", 1925



Subtotal: \$181,500.00 USD
Sales Tax: \$ 0.00 USD
Total: \$181,500.00 USD

Terms

Please reference your invoice number with your payment.
All payments should be made payable to: Jason International Limited.
Title does not pass until payment is received in full.
Shipping, insurance, customs, duties, and/or taxes are the responsibility of the buyer.
Thank you!

Wire transfer information:

ACCOUNT NAME: DIME AND QUARTER INTERNATIONAL LIMITED
BANK NAME: SENG SON BANK HONG KONG, 83 PAPER ROAD CENTRAL HONGKONG
ACCOUNT #: 999-888888-765
SWIFT: ABCDEEE

5. International wires

What is it?

Email account takeover is often used to send an advisor fraudulent wire instructions to deposit the funds into an international bank account. Cybercriminals can be located anywhere in the world, and often the destination for fraudulent funds is overseas. While fraud can occur with any bank recipient, wire recalls are not guaranteed, and funds are much less likely to be returned when sent overseas.

How does it happen?

Fraudsters may direct illegally obtained money directly to an international bank or domestically to several banks before ultimately sending to a foreign bank.

NOTE: Wires are submitted with a SWIFT code in lieu of ABA and can be either delivered in U.S. dollars or exchanged for foreign currency.

These wires may involve:

- Requests for high dollar amounts, i.e., exceeding \$100,000
- Wire instructions submitted with counterfeit documentation such as art invoices or subscription agreements, to make the transaction appear authentic
- International wires to China, Hong Kong and Turkey, which may pose a heightened risk

Example(s)

CNN reports that 83% of wire fraud is directed to banks in China and Hong Kong. While the reason for this is not fully understood, some suspect it's because China doesn't have an extradition policy with the U.S. and will not send its citizens to be prosecuted in American courts.

Tips to prevent or identify

- Follow your standard policies and procedures, but also apply extra due diligence when accepting disbursements to foreign countries.
- Ask your clients: How do you know the beneficiary? How did you receive the instructions (were they sent via email)? Did you personally speak to the recipient?

6. Language cues

What is it?

Email inquiries containing prominent language cues that deviate from common English.

How does it happen?

Cybercriminals can be physically located around the world and often are outside of the U.S. While many criminal rings can employ translators who are fluent in the English language, we still see a high number of email communications that include small spelling errors or grammatical deviations that can signal fraud.

Example(s)

Frequent cues include:

- Use of lowercase "I"
- Words like "kindly," "please advice," "please arrange," "I hope this finds you well"
- Overstated politeness, such as "Have a superb day," "delightful"
- Inconsistent fonts
- Lack of or incorrect punctuation
- Dates on fraudulent documents typed in an international format, e.g., 2017-03-17 14:27:00 (GMT)

Tips to prevent or identify

- Apply additional scrutiny if you see language that deviates not only from common American English but also from the standard tone and writing style of your client.

7. Business email compromise

What is it?

In this sophisticated scam targeting businesses, email requests for transactions can deceptively appear to be sent by a person with authority inside the company.

How does it happen?

An email often urgently asks for funds to be transferred or for a vendor invoice to be paid while the “sender” is not available for verbal verification. Sometimes requests reference a “top-secret” project that should not be discussed with anyone else in the organization. The recipient is persuaded to act on the instructions because they appear to be from someone of authority. Security protocols may be abandoned to comply with the request.

Example(s)

According to this [Federal Bureau of Investigation alert](#), there are five common scenarios for business email compromise:

1. **Businesses working with a foreign supplier**—The business has a long-standing relationship with a supplier and is asked to wire funds to a fraudulent account to pay a bill or invoice via phone, fax, or email.
2. **Business (executive) receiving or initiating a wire transfer request**—The email of a high-level business executive is compromised or spoofed. An urgent email requesting funds is sent to a second employee within the firm, such as someone with disbursement authority in accounts payable.
3. **Business contacts receiving fraudulent correspondence through compromised email**—An employee’s email is hacked and used to send payment requests to firms it supplies with products or provides services for. In reality, when the invoices are paid, the funds go to a fraudster-controlled bank account. It may take weeks or months before both businesses discover the fraud.
4. **Business executive and attorney impersonation**—The fraudster poses as a lawyer or the lawyer’s representative and claims to be handling a confidential matter. The victim may be pressured to act quickly and/or secretly to make a payment.
5. **Data theft**—The fraudster, who is seeking personal information (e.g., names, addresses, Social Security numbers, or salary information) sends a request using a business executive’s compromised email to a second person in the firm responsible for W-2s or maintaining personal information, such as someone in human resources, bookkeeping, or auditing.

Tips to prevent or identify

See the [FBI Internet Crime Complaint Center \(IC3\)](#) for suggestions, including:

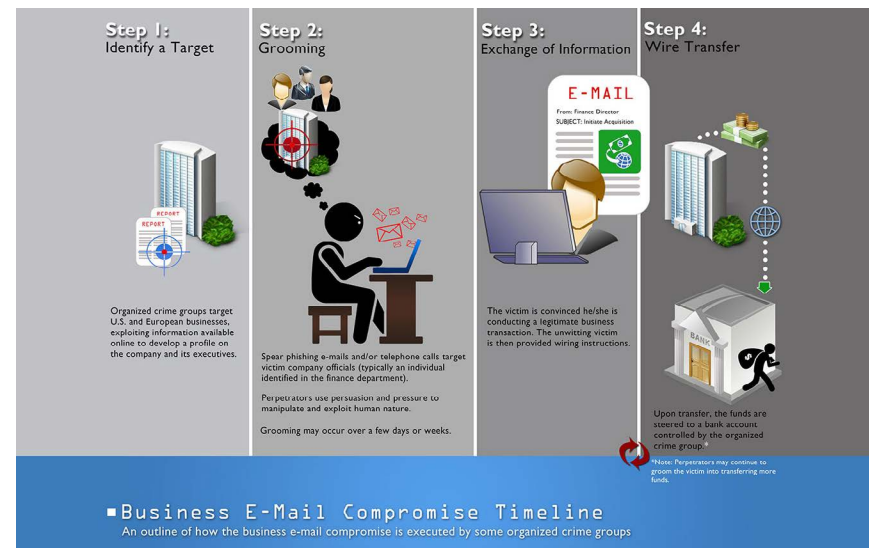
- Rules to detect emails sent from a domain that is similar to (but not exactly the same as) the company’s domain
- Processes for confirming requests for fund transfers internally
- Tips for knowing the habits of your clients and details about their disbursements

Resources:

- [FBI Internet Crime Complaint Center \(IC3\) Alert](#)
- [Cloudmark Security Blog article on “The Top 5 CEO Email Wire Fraud Attacks: Rising in Frequency, Increasing in Financial Losses”](#)

Business e-mail compromise

Cyber-enabled financial fraud on the rise globally



<https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise>

Client impersonation and identity theft

What is it?

Client impersonation or identity theft (ID theft) occurs when one person uses a second person's identifying information to assume his or her identity for the purpose of committing fraud and other crimes.

This category of fraud can be executed through in-person, verbal, or electronic channels, and can be either familial (attempted by a family member) or external fraud (attempted by an unknown party).

Electronic channels are the most prevalent path for ID theft, which can use several different methods and combinations, such as stealing credentials through phishing, malware, and other techniques.

How does it happen?

Client impersonation and ID theft fall into two categories:

1. Low tech methods: This may include deception and **social engineering** where fraudsters pose as a trusted person for the purpose of financial gain or to access information. For example, they may contact a call center or call you directly, posing as the client.

It can also include taking physical possession of devices, ATM cards, financial statements and other materials that contain the client's information.

2. High tech methods: Once fraudsters have the necessary information and access, they may log in to a client's account to gain more information, intercept verification codes, redirect devices, initiate withdrawals, change account information, and more.

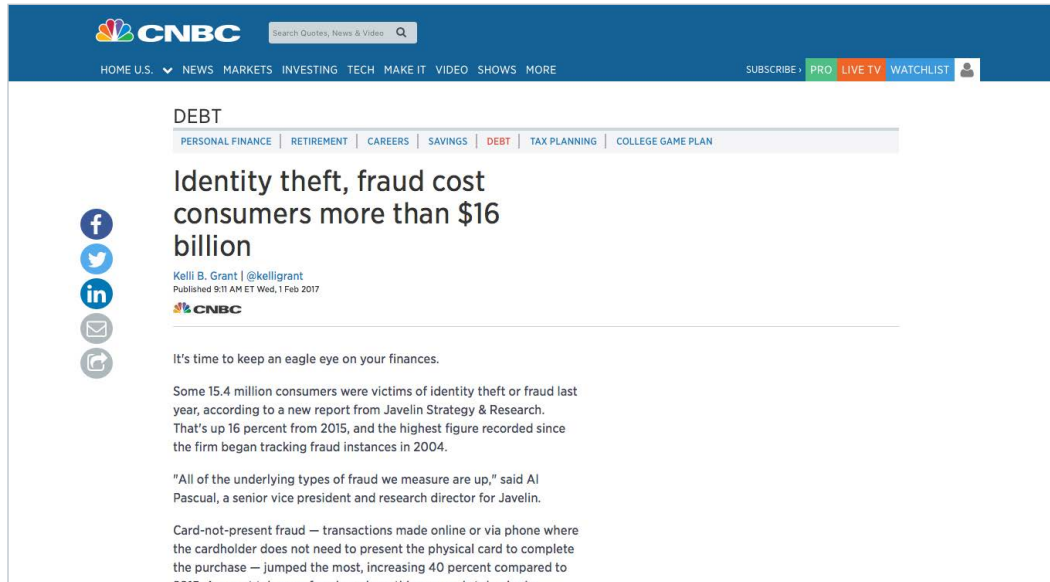
ID theft is a broad topic, so these examples are not all-inclusive and may overlap with other methods that also result in a loss of client information.

Resources

- [FBI Identity Theft page](#)
- [Federal Trade Commission \(FTC\) identity theft resources:](#)
 - [Consumer information](#)
 - [Report and recover from identity theft](#)
- [USA.gov Identity Theft page](#)
- [IRS Identity Protection page](#)

Example

CNBC notes the prevalence and extent of identity theft in 2017, costing consumers more than \$16 billion.



The image is a screenshot of a CNBC news article. At the top, there is a blue navigation bar with the CNBC logo on the left and a search bar in the center. Below the navigation bar, there are several menu items: HOME U.S., NEWS, MARKETS, INVESTING, TECH, MAKE IT, VIDEO, SHOWS, MORE, SUBSCRIBE, PRO, LIVE TV, and WATCHLIST. The main content area has a white background. At the top of this area, the word 'DEBT' is displayed in a large, bold font. Below it, there is a horizontal menu with several categories: PERSONAL FINANCE, RETIREMENT, CAREERS, SAVINGS, DEBT (highlighted), TAX PLANNING, and COLLEGE GAME PLAN. The article title is 'Identity theft, fraud cost consumers more than \$16 billion'. Below the title, the author's name 'Kelli B. Grant | @kelligrant' and the publication date 'Published 9:11 AM ET Wed, 1 Feb 2017' are listed. To the left of the article text, there are four social media sharing icons: Facebook, Twitter, LinkedIn, and Email. The article text begins with the sentence 'It's time to keep an eagle eye on your finances.' followed by a paragraph stating 'Some 15.4 million consumers were victims of identity theft or fraud last year, according to a new report from Javelin Strategy & Research. That's up 16 percent from 2015, and the highest figure recorded since the firm began tracking fraud instances in 2004.' A quote follows: '"All of the underlying types of fraud we measure are up," said AI Pascual, a senior vice president and research director for Javelin.' The text then discusses 'Card-not-present fraud — transactions made online or via phone where the cardholder does not need to present the physical card to complete the purchase — jumped the most, increasing 40 percent compared to 2015.'

<https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html>

Tips to prevent or identify

- Safeguard information and keep personal information secure.
- Consider how you interact with clients via email or phone and be selective about disclosing details.
- Employ strict authentication protocols that you follow for every transaction—no exceptions.
- Educate and train your staff to ensure they are talking to your true client.

Keep reading for more information on specific types of [client impersonation and identity theft](#) »

1. Social engineering

What is it?

Manipulating others to divulge sensitive or private information typically involves an unauthorized individual assuming the identity of a client, or tricking a person into believing he or she is a trustworthy source.

How does it happen?

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 use of manipulation is intended to convince the individual to either release unauthorized information or perform actions for the scammer's benefit, such as sending money.

It is very common for the fraudster to visit social media sites and other sources to obtain identifying information to bolster their credibility and gain more substantial information.

Fraudsters will sometimes rely on human error to obtain additional information. For example, while answering a security question about previous employers, they'll rely on a LinkedIn profile. If the answer is incorrect, the fraudster will guess using the previous employer 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, the customer service rep will 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 am calling from the doctor's office and they require 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?"

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

Example(s)

USA Today highlighted **DefCon**, an annual hackers convention that allows attendees to test their hacking skills. One of the sessions included a social engineering game in which contestants are given 25 minutes to call a real company and use their charm and social influence to obtain private client information from the business' employees. The contest illustrates how easy it can be for a social engineer to successfully persuade employees to disclose information or perform actions to unauthorized parties.

Tips to prevent or identify

- Use caution when sharing information and personal details on social media.
- Limit whom you trust with your and your clients' personal information.
- Be aware of your surroundings when talking on the phone. Do not hold conversations regarding your role or client interactions in public places.

2. Shoulder surfing

What is it?

Shoulder surfing involves obtaining personal or private information through direct observation, such as looking over a person's shoulder to gather pertinent information while the victim is unaware.

How does it happen?

Shoulder surfing is especially effective in crowded places where a person is using a computer or smartphone. Binoculars, video cameras, and vision-enhancing devices also are used, depending on the location and situation.

A common scenario is for a fraudster to watch an account holder conduct a transaction online in a public place and make note of the credentials entered on the victim's device. The fraudster then uses the credentials to access the account illegally.

2. Shoulder surfing (continued)

Example(s)

An account holder withdraws cash at an ATM and enters their PIN, which is seen by the fraudster. As the account holder rushes to catch their train, the ATM asks, “Do you want another transaction?” The fraudster steps in and makes several cash withdrawals.

In another ATM scenario, the fraudster waits until after they’ve seen the account holder enter their PIN. They then distract the account holder, perhaps by saying that a bill fell to the floor. As the account holder bends over to search for the missing cash, the fraudster grabs the ATM card and runs. Since the criminal has the account holder’s PIN, they can quickly visit another ATM and withdraw funds.

Tips to prevent or identify

- Never access your personal accounts or discuss personal information in public.
- Avoid any transactions that require entering of credentials, PINs, or other sensitive information when in public.
- Never share your password or release any vital information to anyone.

3. Spoofing

What is it?

Spoofing is an act of deception where communication appears to be from a trusted source.

There are several variations of spoofing, for example:

- A fraudster leverages a forged email address to imitate a client’s email.
- A phone call that displays the client’s phone number on the caller ID is made to a financial institution.
- IP spoofing, in which a computer appears to be geographically located in one place when it’s actually in another, is also employed by criminals seeking to conceal their geolocation.

Spoofing may be used to gain the trust of the recipient to obtain nonpublic information or request disbursements.

How does it happen?

Spoofing can occur using many methods and technologies. Phone spoofing, for example, is cheap and easy to perform through free apps that make the incoming phone number appear to be the client’s. Email addresses are also free and can be masked or appear to be almost identical and imperceptibly different from your client’s.

Example(s)

Scammers use fake caller ID information to trick you into thinking they are someone local and trusted (e.g., government agency or police department) or a company you do business with (e.g., your bank or cable provider).

Tips to prevent or identify

- Do not rely on the phone number the “client” uses to call you to confirm their identity.
- Adhere to your verification processes when verbally verifying requests.

Resource(s)

- [FTC blog post, “Scammers Can Fake Caller ID Info”](#)

4. Call forwarding and porting

What is it?

In the call forwarding tactic, a consumer's phone number is routed from a legitimate phone number to another number, such as the fraudster's cell phone. This circumvents an institution's call-back process to verify transactions prior to transferring funds.

Like call forwarding, porting occurs when calls are rerouted to a new device. However, in porting the switch is moved to the new device, and the original line is no longer functional.

How does it happen?

Call forwarding/porting can be performed with a phone company through stolen credentials or by social engineering a call center. Fraudsters may use scanners, eavesdropping, cloning phone devices and other technological advances to reroute calls.

Example(s)

This article from Bruce Schneier's *Schneier on Security* blog provides an [example](#) illustrating how call forwarding for a pizza parlor allowed a scammer access to patrons' credit card information.

Tips to prevent or identify

- Do not rely on the phone number used to call you as one of your authenticating tools.
- Apply standard verification processes.
- If your client's calls are being forwarded, attempt to contact your client at alternate numbers, such as their business phone number.
- If you or your client suspect their calls are being forwarded, have them call their phone company or mobile provider directly to escalate.

5. New account fraud

What is it?

Fraudster employs identity theft to open an account in an existing client's name in order to funnel disbursements between accounts and institutions.

How does it happen?

Criminals obtain client information from unauthorized sources, and provide that information to a new institution to open an account that appears to be in your client's name.

Example(s)

See the [Department of Justice](#) website for some examples of recent cases of ID theft and unauthorized new accounts.

Tips to prevent or identify

- Educate your clients on protecting their information through physical safeguards such as shredding important documents and not leaving personal information in public locations.
- Encourage safe cyber practices such as keeping systems up-to-date, being vigilant about defending against phishing attempts, and employing effective password management and wireless network safety.

↔ Identical or first-party disbursements

What is it?

In first-party disbursements, also sometimes called identical registration or like-to-like, fraudsters request money movements to an investment account at a contra bank that is registered in the client's name (identity theft) or to an account at the external bank that appears to be registered in the client's name. This typically occurs via a wire or MoneyLink transfer but can also occur with check requests and transfer of accounts.

This type of fraud is often done to mask the funds' true beneficiary or destination. It may also be an attempt to bypass a financial institution's controls.

How does it happen?

Take the following disbursement as an example:

\$100K wire request:

	From	To
Name	Jane Smith	Jane Smith
Type	Investment account	Bank account
ABA number	N/A	123456789
Account	12345678	1234567



It appears this transaction would not result in a change in ownership. In reality, two fraud scenarios may apply:

1. The fraudster opens a bank account to receive the funds in the client's name—John Doe opened a fake account in Jane Smith's name—in an identity theft scheme. This might have occurred after a data breach in which John Doe obtained enough of Jane's personal information to open a bank account in her name.
2. The receiving account is, in fact, registered to a different name (John Doe) controlled by the fraudster. In this scenario, the fraudster provides disbursement instructions to the investment firm indicating the account is registered in one name (the client's) when it is actually registered in a different name that is controlled by the fraudster.

This can sometimes pass undetected because:

- The Fedwire system is based on numbers, not on registrations or names. A wire can post if the ABA and account numbers match. Not all receiving institutions have processes in place to confirm that the registration noted on the wiring instructions from the delivering bank match what they have on file.
- Due to privacy laws, financial institutions and banks are not able to confirm registration information with the sending institution.

Resources

- [Partnering with your client to reduce risk](#) 
- [Review best practices: Reduce fraud risk when moving money](#)
- [Best practices for conducting client verification calls](#) 

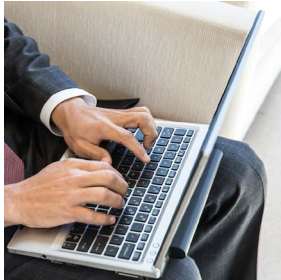
General information on fraud:

- [Association of Certified Fraud Examiners Fraud Resources Library](#)
- [Financial Fraud Enforcement Task Force](#)
- [National Cyber Security Alliance StaySafeOnline](#)
- [FBI Scams and Safety](#)

Case study example

Understanding the threats

Establishing MoneyLink to a same-name account



1. The client's email account is compromised, and their Advisor received fraudulent emails requesting a standing ACH instruction to an identical registered account at a contra firm. Trades were placed to make funds available, and a \$15,000 transfer is requested and processed. No verification call is made to the client. Advisor receives emails from the client's email account requesting a standing ACH instruction to a same-name account at the bank. Trades and a \$15K transfer are requested and processed. No verification call is made to the client.
2. A second ACH request for \$35K is received and accepted via email.
3. The fraudster attempts a third request—a foreign wire—to a same-name account for \$85K. This disbursement placed on hold to obtain client verbal verification. When contacted, the client confirmed all 3 transactions were fraud.

Red flag review

1. Standing instruction set-up followed by multiple disbursement requests
2. Unavailable by phone
3. Emails included grammar/tone cues "kindly," "have a superb day," and "delightful"
4. Signature discrepancies
5. First-party instructions to circumvent third-party controls
6. **Loss:** \$15K plus trade losses; \$35K recalled

This example is hypothetical and for illustrative purposes only

Charles Schwab Advisor Services

Tips to prevent or identify

- Treat first-party disbursements with the same strict scrutiny as you treat third-party money movements.
- Diligently monitor alerts on Schwab Advisor Center®. Watch for client-initiated online transactions. If you see an online disbursement you were not anticipating, call or use video conferencing to directly confirm the transaction with your client.
- During the conversation, have your client confirm where the instructions came from and the details of the transaction. Do not volunteer information.
- Never trust email to conduct business.

Keep reading for more information on specific types of [first-party disbursements](#) »

1. MoneyLink fraud

What is it?

Schwab MoneyLink® profiles are set up between a legitimate client account and an external bank account that is represented as being in the client's name. This external account is actually controlled by the fraudster.

How does it happen?

MoneyLink fraud to alleged like-to-like registrations can occur:

- **Online:** Criminals obtain Schwab or SchwabAlliance.com credentials from end-clients to access the account online. New MoneyLink profiles are established with external bank accounts that appear to be in the client's name.
- **Paper:** Bad actors may also pursue this tactic via a paper-based MoneyLink fraud facilitated by the investment advisor's office through the email channel. The fraudster will forge the client's signature on the MoneyLink form and submit a counterfeit voided check.

New profile instructions are sometimes submitted in conjunction with fraudulent new account openings.

Example(s)

A fraudster gains credentials to Nancy Nickel's account on SchwabAlliance.com and changes the account email address to one controlled by the fraudster. A new MoneyLink profile is set up in Nancy's name at ABC bank, and notifications are sent to the email account controlled by the fraudster. Following profile validation, the fraudster initiates small-dollar transfers in an attempt to fly under the radar, but then enters multiple subsequent requests. The total value of all the combined transfers is substantial.

Tips to prevent or identify

- Watch Schwab Advisor Center® alerts for client-initiated MoneyLink profile setups and contact your client directly if you have questions regarding the activity.
- For advisor-facilitated requests, treat MoneyLink profile setups with the same scrutiny as you treat other third-party disbursements. Incorporate client verification calls into your processes.

2. Wire fraud

What is it?

Fraudsters may request wires that appear to be a first-party (like-to-like) registration at an external bank. The fraudster may assume that the firm performing the transfer out will have less stringent controls if the assets appear to be going into another account owned by the client. Criminals may also request client-initiated wires online to bypass facilitation by an advisor.

How does it happen?

Client-initiated wires are submitted in the same fashion as third-party wire requests, but instructions indicate that the external bank account is in the same client name as the Schwab account.

Example(s)

Consider the following scenario:

A fraudster takes over your client's (Bill Bucks') email and sends you instructions from the account to wire to his first-party account at ABC bank. Because the funds appear to be going to an account in Bill Bucks' name, the advisor submits the wire instructions without additional confirmation or verification.

Two days later, Bill tells the advisor that he did not request the wire.

Subsequently, you discover that the external bank account was in the name of Nancy Nickel and the funds have already been withdrawn.

Tips to prevent or identify

- Watch Schwab Advisor Center alerts for client-initiated wires and contact your client directly if you have questions regarding the activity.
- For advisor-facilitated requests, treat first-party wires with the same scrutiny as you treat other third-party disbursements. Incorporate client verification calls into your processes.

3. Check fraud

What is it?

Criminals submit instructions to have a check issued from an account in the name of the client and request it be sent to the address on record. The fraudster then physically intercepts the check with the intent to cash or later deposit it.

How does it happen?

The physical delivery of the check is intercepted by the fraudster using different mechanisms:

- Contacting the mail delivery service with instructions to reroute overnight delivery to a different address
- Submitting a change-of-address request with the mail delivery service
- Physically stealing the check from the client's mailbox

Once the fraudster has physical control of the check, it is deposited into an account under their control using various techniques:

- Fraudulently opening an account in the client's name
- Endorsing a check by using "pay to the order of"
- Duping a check-cashing establishment
- Check washing or modifying the check to reflect a different amount or payee

Example(s)

Between March and May 2017, Schwab uncovered a fraud scheme in which over 17 different fraud attempts were tied to the same perpetrator. This bad actor used forged Letters of Authorization and impersonated several clients during multiple calls to Schwab.

Using the names and personal information of Schwab clients (ID theft), the unknown individual fraudulently opened accounts that he now controlled and requested first-party wires from the Schwab account to the newly opened accounts at the external banks.

In other scenarios, he requested checks from Schwab that were drawn on the client accounts. In these instances, he submitted change-of-address instructions to the U.S. Postal Service or provided the overnight carrier instructions to reroute the delivery of the checks. Once in physical possession of the checks, he attempted to cash them at check-cashing stores.

Tips to prevent or identify

- Watch Schwab Advisor Center® alerts for client-initiated transactions and contact your client directly if you have questions regarding the activity.
- For advisor-facilitated requests, treat checks in the client's name with the same scrutiny as you treat other third-party disbursements. Incorporate client validation calls into your processes.

4. Transfer of account (TOA) fraud

What is it?

In this technique, an Automated Customer Account Transfer (ACAT) is initiated with a contra firm. TOA fraud is often paired with unauthorized online account opening at the other firm.

How does it happen?

Stolen information is used to create a new account at a firm. An ACAT transfer is typically initiated with the new account via the online channel, requesting assets from an existing account in your client's name. Funds are then transferred and extracted from the new account.

Example(s)

To understand more about the ACAT system, visit [FINRA online](#).

Tips to prevent or identify

- Monitor Schwab Advisor Center® for alerts of client initiated outgoing transfers that you were not anticipating.
- Call your client every time you see an unfamiliar request.
- Suggest that clients add a credit lock or freeze to limit the chances of accounts being opened at other financial institutions.

Phishing

What is it?

Criminals pretend to be a trustworthy source, using media such as email, phone calls, texts, advertisements, websites, and more to mask their identity to acquire sensitive personal information such as usernames, passwords, Social Security numbers, and credit card details. Phishing can also be used to install **malware** on a system.

Some variations of phishing, based on the channel used, include:

- **Vishing** – Voice phishing, uses **social engineering** over the phone to gain client information.
- **Smishing** – Also known as SMS phishing, smishing uses text messages to send malicious links/attachments or gather personal information.

Typically the objective of the phishing attack is to obtain information to enable ID theft and fraud. The intent of a phishing attempt may not be to perform fraud immediately, but to wait for a fraud opportunity days, weeks or months down the road. In fact, sometimes the fraudster won't even use the information and will instead sell it for profit on the dark web.

Most recently we've also seen phishing attempts that leverage other channels that were not typically used in the past, such as social media, making the threat even more widespread.

How does it happen?

Fraudsters disguise themselves as trusted sources and deceive victims into performing actions that may result in loss of private information or funds or susceptibility to malware.

Example(s)

DocuSign reported a malware phishing attempt stemming from a recent DocuSign data breach in which names and email addresses were compromised. Attackers continue to use this information to send emails to DocuSign users with important-sounding subject lines:

Completed [domain name] – Wire transfer for [recipient name] Document Ready for Signature

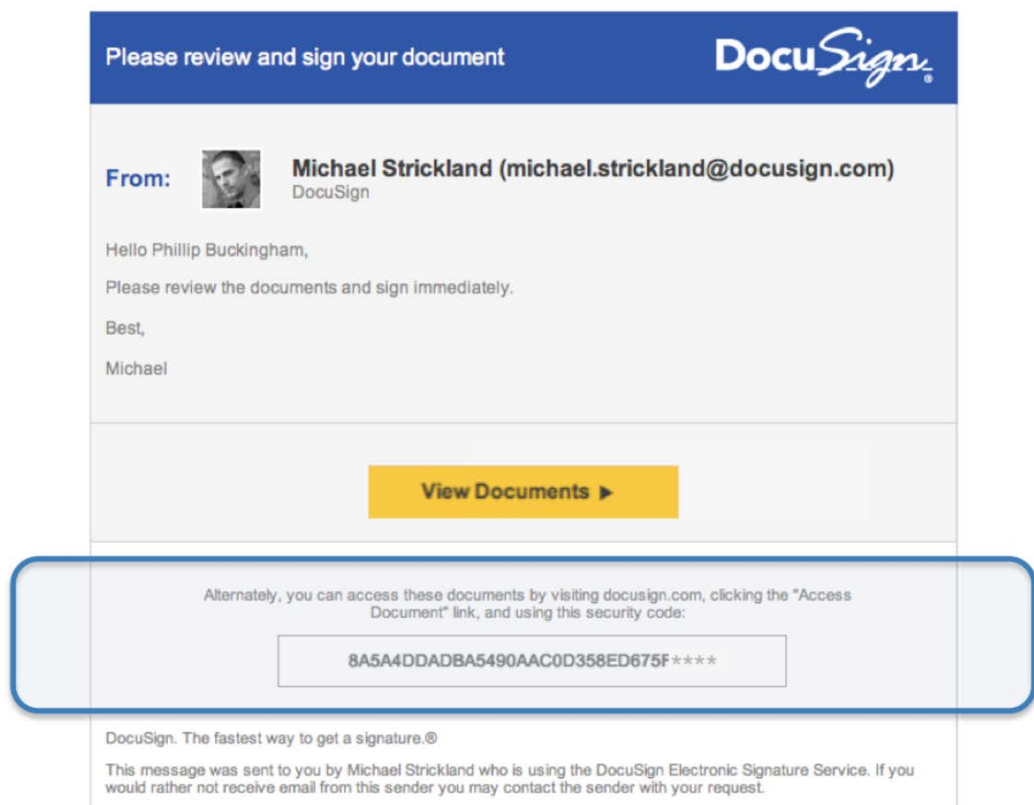
Completed [domain name / email address] – Accounting Invoice [number] Document Ready for Signature

When a user opens the email to investigate, they find an attachment. If the user clicks the attachment to view the contents, it deploys malware:

Resources

- [The Security Awareness Company](#)
- [FTC Consumer Information](#)
 - [Phishing](#)
 - [OnGuardOnline](#)
- [Phishing.org](#)
- [APWG](#) (formerly known as Anti-Phishing Working Group)
- [StaySafeOnline Spam and Phishing](#)

Forward phishing emails to spam@uce.gov, [AWPG](#) and reportphishing@antiphishing.org along with the company that was impersonated.



<https://trust.docusign.com/en-us/personal-safeguards/fraudulent-email-websites/>

Tips to prevent or identify

- Do not click on links or attachments included in emails and texts.
- Hover over links or requests to click to see the true URL.
- Be suspicious of emails that have grayed out CC and To lines, as they may have been sent to a mass distribution list.
- Review the sender's domain to see if it matches the sender's expected domain.
- Deploy spam filters.
- Do not enter your username and password on a web page if you clicked a link or copied and pasted an address within an email to access the page. Instead, enter the address directly into your browser to visit the trusted website where the account is held to log in as usual.

Keep reading for more information on specific types of [phishing](#) »

1. Spear phishing

What is it?

Spear phishing is directed to a specific person or small group of people.

How does it happen?

This approach is often customized and tailored to a specific person, group, or team, increasing the chances of success. The attempt may include a link to a business or site that is familiar to the user, luring the individual into a false sense of trust.

Example(s)

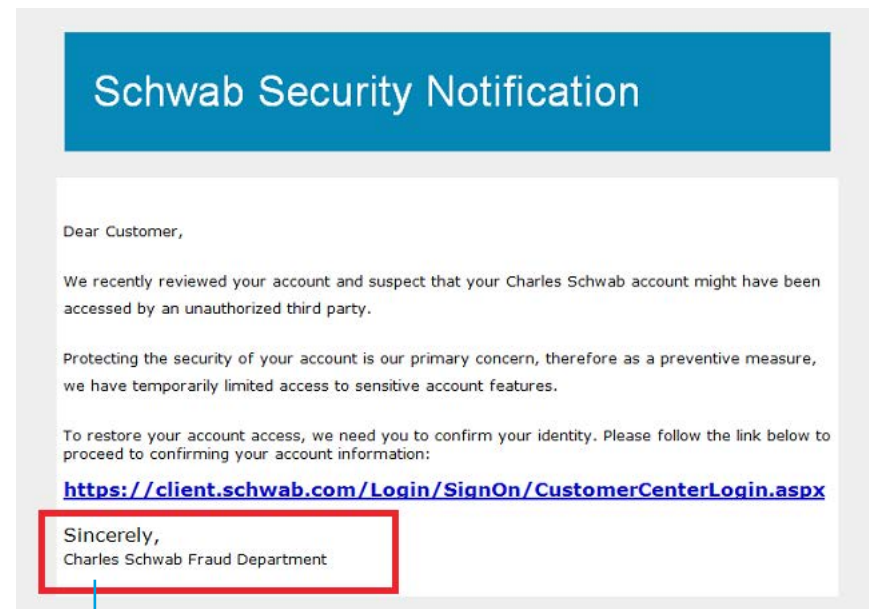
You may have heard [National Public Radio's All Things Considered](#) story or read [Wired magazine's article](#) about the hack into the Democratic National Committee's files by two independent groups of hackers based in Russia. One group's standard tactic is to use spear phishing emails to gain credentials by getting the recipient to click on spoofed websites. While it's not yet been determined if that was the strategy used in this attack, it is likely. The hackers accessed the Democrats' correspondence, including emails, and research on the Republican opponent, Donald Trump, for an extended period, potentially a year.

We've seen spear phishing attempts targeting Schwab clients too. Earlier this year some clients received a fake email, right, that looked like it was coming from Schwab's fraud department. If they clicked the link, the recipients were taken to a spoofed Schwab website that prompted them to enter their personal information, which the fraudster could use for their benefit.

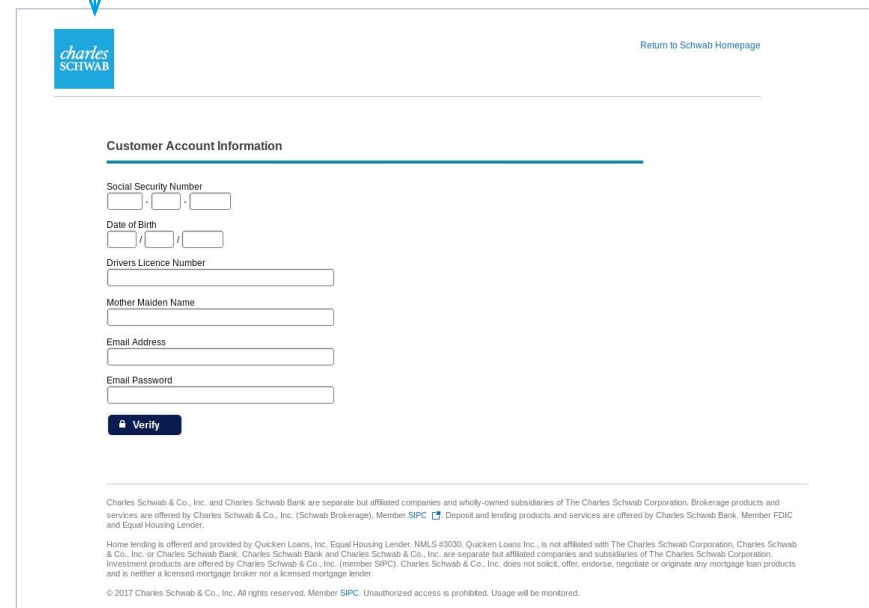
NOTE: If you or your clients receive an email from Schwab that appears to be phishing, escalate to your Service Team. Schwab's phishing department will investigate and take down any fraudulent websites.

Tips to prevent or identify

- Do not click links or attachments included in emails or text messages.
- Hover over links to view the URL.
- Be suspect of emails that have grayed out CC and To lines, as they may have been sent to a mass distribution list.
- Review the domain of the sender to see if it matches the sender's expected domain.
- Deploy spam filters.
- Do not enter your username and password on a web page if you clicked a link or copied and pasted an address within an email to access the page. Instead, enter the address directly into your browser to visit the trusted website where the account is held to log in as usual.



Clicking on the link opens the second screen.



2. Whaling

What is it?

This variation on spear phishing is targeted at high profile, high-net-worth individuals such as corporate officers, politicians or celebrities.

How does it happen?

Whaling attacks are perpetrated using methods similar to spear phishing but are highly individualized. The objective is to trick an individual to fall for the phishing attempt by enticing them to click links or download attachments that install malware onto the person's device.

One motive for whaling may be to obtain the high-profile person's email credentials to enable email account takeover. The hacker may then use access to the email account to perform other types of fraud, such as [business email compromise](#).

This tactic can also be a generic email, without links or attachments, to convince the recipient to respond to the attacker and release personal information or funds.

Example(s)

Emails spoofing as an official legal, regulatory, or other executive issue may be directed to the CEO or another officer of a company. The email instruction includes a link to view the official document that installs malware if clicked.

Tips to prevent or identify

- Do not click on links or attachments included in emails and texts.
- Hover over links or requests to click to see the true URL.
- Be suspect of emails that have grayed out CC and To lines, as they may have been sent to a mass distribution list.
- Review the domain of the sender to see if it matches the sender's expected domain.
- Deploy spam filters.
- Do not enter your username and password on a web page if you clicked a link or copied and pasted an address within an email to access the page. Instead, enter the address directly into your browser to visit the trusted website where the account is held to log in as usual.

3. Clone phishing

What is it?

A legitimate email that was sent previously and contains links, an attachment, or both is copied, and the links and attachments are replaced with malicious ones.

How does it happen?

The content from a legitimate email is copied and sent to the same email recipient. The original links and attachments are replaced with malicious ones that, if clicked, install malware onto the recipient's device. Because the email was legitimate to begin with, it appears to be from the original sender.

Example(s)

Emails may be sent from what appears to be a familiar merchant, confirming a purchase that was recently made with a link to click for a status update. The email may be a clone from a previous order confirmation; however, if the link in the new email is clicked, it deploys malware.

Tips to prevent or identify

- Do not click on links or attachments included in emails and texts.
- Hover over links or requests to click to see the true URL.
- Be suspect of emails that have grayed out CC and To lines, as they may have been sent to a mass distribution list.
- Review the domain of the sender to see if it matches the sender's expected domain.
- Deploy spam filters.
- Do not enter your username and password on a web page if you clicked a link or copied and pasted an address within an email to access the page. Instead, enter the address directly into your browser to visit the trusted website where the account is held to log in as usual.

4. Social media phishing

What is it?

Social media phishing is a broad term that covers many types of illegal acts designed to convince you that the fraudster can be trusted.

Fraudsters typically scour social media sites to harvest information with the intent of committing malicious acts. They can then pretend to be your friend or reach out to your contacts while impersonating you.

There is also a wide assortment of digital threats that the criminal implants on the sites to entice you to click. Social media phishing attacks have increased 500% in 2017, and Facebook is, by far, the top mechanism for delivering malware.

How does it happen?

Fraudsters send the victim a crafted email that contains convincing personal details that make it appear to be coming from a friend.

They can also imitate the target to trick their contacts. Copying a person's Facebook profile and sending emails to friends requesting they accept the request is an example.

Some tactics in the diagram at right we've already covered; others are defined below:

Clickjacking: Your friend posted a picture of a kitten on their Facebook page. You think you're clicking to see the related video, but you've just downloaded malware or are taken to a fraudster's site.

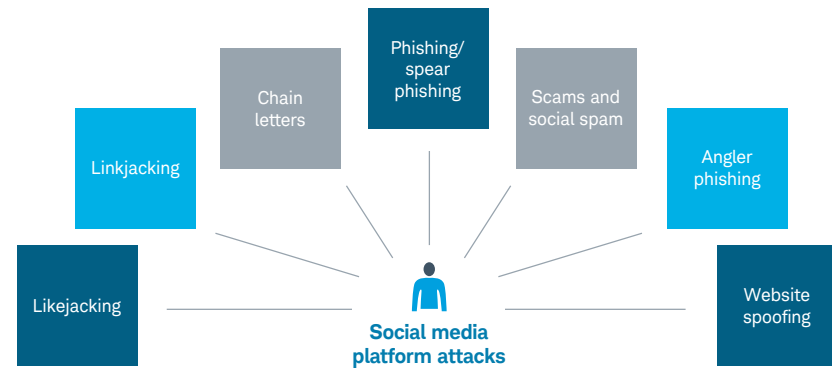
Likejacking: This is a variation of clickjacking, where you click a "like" button on Facebook.

Linkjacking: You are redirected from one website's links to another. This can drive traffic to the alternate content and generate money on any click-through ads.

Chain letters: Chain letters can be distributed in a variety of ways, including email, an instant message, a posting on a friend's social network profile or a text message. They ask you to perform a very small action to avoid a negative consequence or to receive a reward. You've probably seen these: "Send this email to 10 people, and you will receive a gift card to a popular retailer" or "Bill Gates is sharing his fortune, and all you have to do is forward this email." Some are harmless, but others can be malicious.

Social spam: This type of spam uses a fake social media account that you may trust in order to do things such as share undesired or excessive content, post fake positive reviews, or spread malicious links.

Digital threats of social media



Angler phishing: Impersonators register fake Twitter accounts that masquerade as customer support. The imposter sends fake messages, such as asking users to click for assistance with an urgent matter, or monitors real support accounts for irate customer messages and quickly jumps in to steal credentials or send back messages to users loaded with malicious links.

Website spoofing: Fraudsters publish a fake website with the intention of misleading readers that the website has been created by a different person or organization. Normally, the spoof website will adopt the design of the target website and sometimes have a similar URL.

Example(s)

PhishMe's [Phishing and Social Media infographic](#) provides more information and some examples.

Tips to prevent or identify

- Strengthen your security settings.
- Do not post personal information to social media.
- Close old social media accounts.
- Turn off the GPS function on your mobile devices.
- Do not accept friend requests from people you don't know or repeat requests from people to whom you're already connected.
- Create strong and unique passwords for your social media accounts, and change them frequently.

Scams

What is it?

A scam is a fraudulent scheme orchestrated to swindle an individual out of money or possessions by convincing the victim to fall for false pretenses. In a scam, a victim willingly complies with the scammer's request by sending money or providing information under the belief it is for a different purpose or to a trusted recipient.

How does it happen?


Bad actors will approach persons of interest using various channels, such as email, phone, text, or mail. Scammers will pose as trustworthy sources who convince an individual to perform an action to benefit the perpetrator, such as sending or accepting funds.

Scams frequently target an unwitting money mule, sometimes referred to as a “smurfer,” who transfers money acquired illegally (e.g., stolen) in person, through a courier service, or electronically on behalf of others. This individual, often an unwitting victim of a scam, acts as an accomplice in a fraud scheme to move illegally received funds from one source to another. For example, in the romance scam scenario, a victim may accept funds at the request of their “sweetheart” and agree to resend the funds to another recipient account likely controlled by the scammer.

Tips to prevent or identify

- Standard client verification processes may not completely safeguard against scams, but this is something you should look out for on your client's behalf. Conversations about the transfers should go beyond just confirming you're speaking to your client. For example:
 - Ask questions about where the client is sending money and why—especially if this is not typical of your client's past behavior, if these are new instructions or if the funds are going to a new recipient.
 - Encourage clients to verbally verify transfer instructions with the recipient and to ask for supporting documentation.
 - Suggest clients view goods or merchandise in-person before agreeing to purchase.
 - Consider using services that have purchase protection and / or an escrow service until both parties agree the transaction is satisfactory, especially for high-dollar transactions.

Resources

- [Schwab's Cybersecurity Resource Center](#) 
- [FBI Common Fraud Schemes](#)
- [Fraud.org Common Scams](#)
- [FTC Scam Alerts](#)

- Recommend clients conduct online searches, check with the Better Business Bureau and perform other due diligence in confirming the legitimacy of the offer.
- Determine if your client understands the details of the request or the transaction.
- Have clients exercise caution when determining the method for submitting payments. For example, fraudsters often request currency such as bitcoin, gift cards, and prepaid debit cards. Remember, if an international wire is deemed fraudulent, it is typically difficult to recall.

Case study example

Understanding the language of a scam

The client used an online career website to search for a new job and was interviewed by the fraudster over the phone.

The fraudster, purporting to be the client's online manager, told the client that she had landed the job and began to engage her in an effort to help facilitate fraudulent money movement activity. The fraudster told the client that she would need to send a wire to pay for special equipment before starting her new job as a virtual guidance counselor.

The client contacted her Advisor and asked if he would assist with freeing up cash in her account for an outgoing wire. The Advisor asked the client for more information regarding the transaction, and the client said that she had landed a new job and needed the money before she could start.

At this point, the fraudster began to use the client as a money mule. He contacted the client to make her aware that he would need her assistance with making payments to company vendors. The fraudster asked the client to open a personal account with Bank of America, and she provided her Schwab account username and password to the fraudster.

The fraudster made several mobile check deposits in the client's Schwab account, and the checks were returned after being identified as counterfeit. Additionally, the fraudster initiated several outgoing third-party wires from the client's Schwab account to the new Bank of America account. The fraudster instructed the client to transfer funds from the Bank of America account via a wire and to deposit cash from the account into accounts at several financial institutions.

The client was not aware that she had been the victim of an internet scam or that she was being used as a money mule to facilitate fraudulent transactions and assist with possible criminal activity.

The client suffered a \$9,000 loss from this incident.

1. Properties

What is it?

Under false pretenses, property is offered for rent or purchase, including vacation rentals with known scams posted on sites such as Airbnb, VRBO and Craigslist.

How does it happen?

Scammers will post nonexistent properties for purchase or rent. The bad actors will insist on receiving a down payment or full purchase price while providing excuses, denying a physical viewing, showing a different property, or failing to produce supporting documentation.

Another version of a rental scam targets property owners. A renter or buyer will approach you and agree to submit a down payment for the property via check. The deposit is “accidentally” made for an amount larger than the payment requirement. The renter or buyer requests that you send the amount of the overpayment immediately. The overage amount is sent to the fraudster, whose initial check fails to clear. The property owner cannot recover the deposit or the overage funds.

Example(s)

In this May 2017 *Country Living* article titled “[There’s a New Craigslist Scam Targeting Homeowners and Renters](#),” a homeowner shares how a scammer posed as a landlord and created a listing to rent her house without her knowledge.

Tips to prevent or identify

- Don’t provide forms of payment for properties, landlords, or owners not seen or met in person.
- Beware of deals that appear too good to be true.
- Be cautious of vendors who request money early in the transaction.
- Obtain a full contract before sending money.

2. Romance/marriage/sweetheart/catfishing

What is it?

One of the most common scams is associated with online dating. Fraudsters trick victims into falling in love by posting false bios and personas online to convince victims to send money or accept money as a mule.

How does it happen?

False profiles are established on online dating sites, often with pictures of real people stolen from social media. The scammers engage with victims employing typical tactics:

- Asking a lot of personal questions to help the scammer model responses that appeal to the victim
- Quickly wanting to communicate off the dating website and through personal email or text instead
- Falling in love quickly with the victim
- Insisting they want to meet but consistently coming up with excuses
- Often claiming they have no immediate family to turn to for assistance

Once an emotional attachment is established, the scammer will come up with an elaborate financial crisis to get the victim to either send money or accept a check on behalf of their paramour for further distribution to an account controlled by the scammer.

Example(s)

The FBI released a story about a woman who fell victim to a romance scam by connecting with “Charlie,” a “friend of a friend,” on Facebook. After establishing a strong emotional connection, the scammer persuaded the woman to wire \$30,000 to “finish up a (construction) job” in California. Over the course of two years, she complied with several additional wire requests. Her financial advisor became concerned about the ongoing depletion of funds, and the FBI opened an investigation. She lost \$2 million.

Two accomplices—imposters who posed as South African diplomats who approached the woman to collect funds on Charlie’s behalf—were eventually arrested, but Charlie remains at large.

Tips to prevent or identify

- Perform a Google image search with the person’s profile picture.
- Be cautious of new profiles set up within the past few days.
- Do not send money to an individual you’ve never met in person.

3. Investments/goods/services

What is it?

Investments, goods, or services that either don't exist or are falsely represented are offered for purchase.

How does it happen?

These types of scams can be perpetrated in many ways:

- Ponzi schemes are false investment scams that are performed by offering investments that are funded by early investors and cashed out with the contributions of later investors.
- Promissory notes, precious metals, loans, annuities, and other investment opportunities that either don't exist or are misrepresented are sold.
- Pump-and-dump schemes occur when the market is manipulated by giving recommendations to buy a stock in large quantity based on dishonest information. The stock, already held by the scammer, is sold once the stock price is falsely elevated.
- Goods offered through marketplaces like Craigslist or eBay can target both buyers and sellers.
 - Buyers are tricked into purchasing goods that don't exist or are not in the condition promised.
 - Sellers are given counterfeit payments.
- Scams promise services for a deposit up front followed by a lack of follow-through with the services

Example(s)

Refer to the [FBI Common Fraud Schemes](#) page to keep up-to-date with current scams.

Tips to prevent or identify

- Do not hesitate to ask many questions. Performing due diligence with any investment, good, or service is key to mitigating the risk of a scam.
- For transactions over a certain dollar amount that you are not willing to lose:
 - Insist that you physically inspect the item you are purchasing before depositing any funds or paying.

- Obtain formal documentation on the product or item in question, such as an independent appraisal performed by an expert hired by the buyer.
- Require that the seller provide proof of their identity.

- Perform Internet searches on the person or service in question. However, do not rely solely on positive reviews or recommendations, as they may be false or fabricated.

4. Prizes/lotteries

What is it?

A fraudster attempts to lure the target into believing they are the recipient of a nonexistent sweepstakes, a prize, or money that will be rewarded upon payment of fees or taxes.

How does it happen?

Attempts are made via various channels (e.g., phone, direct mail, pop-up online ad, or email) to a consumer advising them that they are the recipient of a lottery or a substantial prize. To receive the winnings, the individual must first pay a fee for processing or taxes. The prize does not exist.

Alternatively, a target may be mailed a check said to be funds from a sweepstakes or other prize. The victim is directed to deposit the funds and immediately wire a portion of it back to cover the fees and taxes, only to find out later that the check was counterfeit.

Example(s)

Facebook is one of the emerging channels for this type of fraud. An example may include receiving a friend request, either an unknown individual or someone spoofing someone you know, informing you of the winnings. To further engage recipients, they are provided instructions of where to send processing fees or taxes to acquire the prize.

Tips to prevent or identify

- Apply extreme caution before responding to any type of alleged winning as it is most likely a scam.

5. IRS

What is it?

This scheme involves scammers contacting individuals by phone or email and demanding immediate payment of taxes owed, by either wire or prepaid debit card. Alternatively, individuals may be informed they are entitled to a large tax rebate and need to provide their banking information for the credit.

How does it happen?

Fraudsters are employing spoofing techniques to make calls appear to come from the IRS. They may also establish spoofed emails or websites. Operations have been known to originate from call centers based in India whose sole function is to place calls to unsuspecting targets.

Example(s)

See the [IRS Tax Scams / Consumer Alerts page](#) for ongoing updates on tax scams.

Tips to prevent or identify

Exercise caution and be familiar with IRS practices:

- The IRS never calls taxpayers, nor will they ever request credit card, debit card or bank information over the phone.
- The IRS will not require payment via prepaid debit or gift cards.

Resource(s)

- [IRS Security Awareness Tax Tips](#)

6. Payments

What is it?

Scammers worldwide often request funds using methods that facilitate a quick and anonymous payout such as bitcoin, a popular digital currency or “cryptocurrency.” Bitcoin transactions are recorded in a public ledger, but the identity of the requestor is not visible.

Payments may also include other channels that can be used in the same way as cash, such as debit cards, gift cards, or money orders.

How does it happen?

Fraudsters often request that funds be transmitted through bitcoin currency due to the anonymity and ease of transactions. Historically, bitcoin has been used in the darkweb or darknet marketplace for illicit activity, such as the purchase of illegal goods and services or stolen information. Bitcoin is hard to detect, not centralized, fast, and treated almost like cash.

Prepaid debit cards, gift cards, and money orders may also be requested, since funds cannot be traced back to an individual. Prepaid debit cards specifically function like standard debit cards but are not backed by a bank account and offer no protections from fraud.

In all cases, the transmission of funds is anonymous, and the chance of fund recovery by the victim is unlikely.

Example(s)

In addition to scams, bitcoin is also very popular in ransomware attacks, in which the threat is to pay quickly or lose all your data. In the highly publicized WannaCry (aka WannaCrypt) virus attack in May 2017, scammers demanded approximately \$300 to \$600 in bitcoin to restore computer access.

Tips to prevent or identify

- A request for any of these payment options should be a red flag and trigger a thorough examination to determine if fraud is being attempted.

Other cybercrime techniques

What is it?

Crimes, typically financial, are perpetrated through intrusion of computers or other network-connected devices. These cyberattacks are orchestrated by using a wide assortment of tools to compromise networks and devices and are performed for the purposes of illegal access of information such as non-public information, criminal acts such as account or funds takeover, espionage, or other malicious acts.

How does it happen?

Cybercrime can occur through hacking, malicious software/malware, ID theft, and other techniques to target individuals, assets, and governments.

While the cybercriminals who perpetrate this type of fraud may be freelance technologists, they are often part of a larger group of organized crime. Consider it a billion-dollar enterprise, comprised of very specialized roles to develop, administer, and sell cyber intrusion tools and techniques.

Example(s)

Here is a visual representation of the type of criminal groups and the roles that support them



Resources

- [FBI Cyber Crime](#)
- [Schwab's Cybersecurity Resource Center](#)

Tips to prevent or identify

- Employ safe use of software, activating firewalls and keeping systems updated.
- Enable browser security settings.
- Employ safe use of wireless networks.
- Practice effective password management, such as password managers and two-factor authentication.
- Educate yourself and others about top fraud trends.
- Be cautious with emails, including attachments and links from unknown sources.
- Monitor account activity regularly.
- Only keep data on a need-to-know basis, and encrypt sensitive data.
- Educate your staff, teach them how to identify the red flags, and make sure they understand how important cybersecurity is to your firm's brand.

Keep reading for more information on specific types of [other cybercrime techniques](#) »

1. Malware

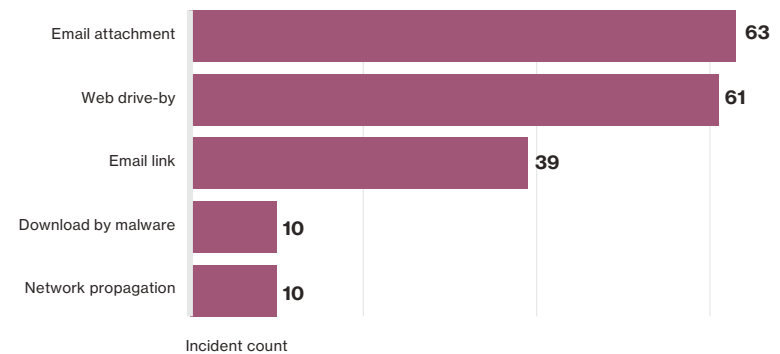
What is it?

Malicious software is installed on a device to gain access to private information or to disable or damage operating systems. There are many variations of malware that include but are not limited to:

- Ransomware – A type of malicious software threat that actors use to deny access to systems or data, holding it hostage until the ransom is paid
- Rogue security software – Malware disguised as antivirus software that misleads customers into believing they have a virus
- Trojan horse – Any type of malware that disguises its true intent by appearing to be something useful
- Road apple – Malware that feeds off human curiosity (e.g., Disks, flash drives, or other removable media are physically placed in a location that lures a victim to access it and then install the software.)
- Keyloggers or screenloggers – Systems that track keyboard strokes or computer navigation and allow hackers to see the private information you input
- Virus – A program that needs a host (file or program) in order to attack and insert itself into another program
- Worm – Like a virus but does not need a host to spread; standalone software
- Spyware – Software that is installed on a device to monitor personal information and device activities

How does it happen?

Malware is installed using a myriad of methods, such as physical installation, the use of phishing with unsafe links, false advertisements, and faked websites. While there are several mechanisms for installing malware, the most prevalent source is phishing attacks with email attachments. These are the top five malware vectors within crimeware according to the 2016 *Verizon Data Breach Investigations Report*:



Example(s)

- **Virus** – In 2000, the “ILOVEYOU” virus was launched. The unsuspecting recipient clicks on the email attachment, spreading the virus to everyone in his contacts list and overwriting all his email files.
- **Trojan horse** – One of the most infamous malware ever launched was a Trojan horse called Zeus. It recorded and stole login credentials for thousands of large multinational corporations and banks, enabling the hackers to steal nearly \$100 million, primarily from U.S. accounts.
- **Malware worm** – In July 2015, a worm called Code Red attacked computers running Microsoft’s IIS web server. It exploited a buffer overflow problem in the operating system. It then infected the computer and began duplicating itself until it drained the system’s resources.
- **Ransomware** – In May 2017, media outlets were filled with reports of a ransomware attack called WannaCry or WannaCrypt. The attackers threatened to destroy files and render the computer useless unless they were paid \$300 to \$600 in bitcoin to recover the computer’s data. Every 72 hours, the ransom would increase if it was not paid.

Other recent attacks in various industries include:


- [US Libraries Hit by Ransomware Attack](#) (January 24, 2017)
- [Emory Healthcare Hit by Ransomware, Data of Over 200,000 Patients Hacked](#) (January 6, 2017)
- [Ransom Attack Hit San Francisco Train System](#) (November 28, 2016)

1. Malware (continued)

Tips to prevent or identify

- Do not download programs from unknown sources, and follow safe phishing practices (e.g., use caution when opening links and attachments).
- Ensure you keep your operating systems and browsers up-to-date with the latest fixes and patches.
- If your computer system does become infected with ransomware, many experts recommend that you do not pay because the chance of getting your files back is minimal. Instead, invest in the Backup 3-2-1 method prior to an attack:
 - 3 backups of any critical files should be created
 - 2 or more formats should be used to store the files, such as DVD and memory stick or the cloud
 - 1 of the backups should be retained off-site

Resources

- Schwab's [Cybersecurity Training: Safeguarding Our Firm and Client Assets](#)  employee training deck
- [PhishMe Ransomware Resource Center](#)
- [FBI Ransomware Prevention and Response for CEOs brochure](#)
- [STOP. THINK. CONNECT. Ransomware Facts & Tips sheet](#)

2. Wi-Fi connection interception

What is it?

This attack uses public Wi-Fi to intercept personal information such as nonpublic information or credit card numbers through compromised network connections.

How does it happen?

It can happen a few ways:

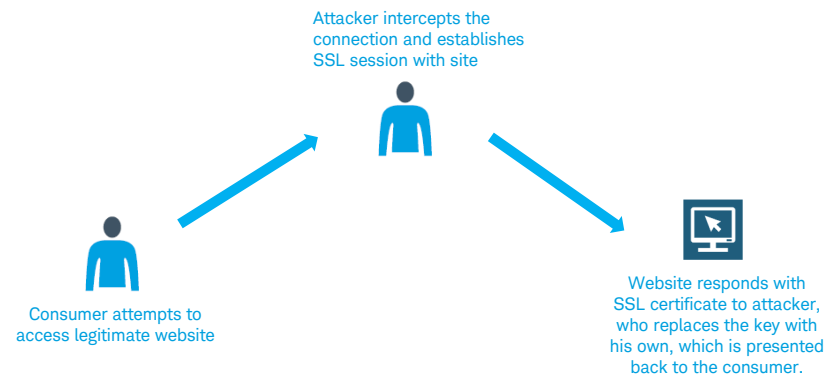
- A “man in the middle” attack essentially allows a hacker to “sit inside your browser” to record what you are doing for the purposes of monitoring and recording credentials or other valuable information you enter. The criminal sits in the middle between you and your service, allowing them to intercept user traffic before it reaches the intended server while presenting you with their own version of the site.
- Using “evil twin” programs, or fake Wi-Fi connections, hackers can intercept sensitive data as it is transmitted wirelessly or received from your laptop or handheld device. This happens when a user connects to what appears to be a free Wi-Fi spot but is actually a rogue access point set up by a hacker who is providing

the network on their connection. Using the compromised Wi-Fi gives the hacker access to your online activity.

- Sniffer software lets a cybercriminal view traffic passing through a network interface. It allows the criminal to take a snapshot of the data being transferred.
- A common tactic is to intercept emails that contain usernames and passwords.

Example(s)

Below is an illustration of the “man in the middle” technique:



Tips to prevent or identify

- Be aware of your surroundings as you work in public places.
- Remember to use encryption programs and to disable network applications whenever working in public.
- Disconnect any features that automatically connect you to outside networks as you travel.
- Avoid accessing public Wi-Fi, and use only wireless networks that are protected.
- If you must use public Wi-Fi, do not accept software updates when connected.
- Install a virtual private network (VPN) or use a personal Wi-Fi hotspot for network access in public locations.
- Use two-factor authentication.

Resource(s)

- [STOP. THINK. CONNECT. Privacy tips for using public computers and wireless networks](#)

3. Data breaches

What is it?

Incidents in which sensitive, personal information or data is stolen by an individual, group, or system. Some prominent, recent data breaches include Target, Yahoo, Comcast, Verizon, and LinkedIn.

How does it happen?

Data breaches can occur in many ways. Some include:

- Physical loss of device
- Malware
- Hacking tactics
- Inside attacks

At right is an illustration of the “who” and the “how” of data breaches, according to Verizon’s *2018 Data Breach Investigations Report*.

Who’s behind the breaches?

73% perpetrated by outsiders

28% involved internal actors

2% involved partners

2% featured multiple parties

50% of breaches were carried out by organized criminal groups

12% of breaches involved actors identified as nation-state or state-affiliated

Who are the victims?

24% of breaches affected healthcare organizations

15% of breaches involved accommodation and food services

14% were breaches of public sector entities

58% of victims are categorized as small businesses

What tactics are utilized?

48% of breaches featured hacking

30% included malware

17% of breaches had errors as causal events

17% were social attacks

12% involved privilege misuse

11% of breaches involved physical actions

What are other commonalities?

49% of non-POS malware was installed via malicious email

76% of breaches were financially motivated

13% of breaches were motivated by the gain of strategic advantage (espionage)

68% of breaches took months or longer to discover

3. Data breaches (continued)

Example(s)

Announcements of new data intrusions hit the news daily, revealing that no company is safe. At right is an illustration of known data breaches and the type of information obtained with each incident.

Tips to prevent or identify

For you and your clients:

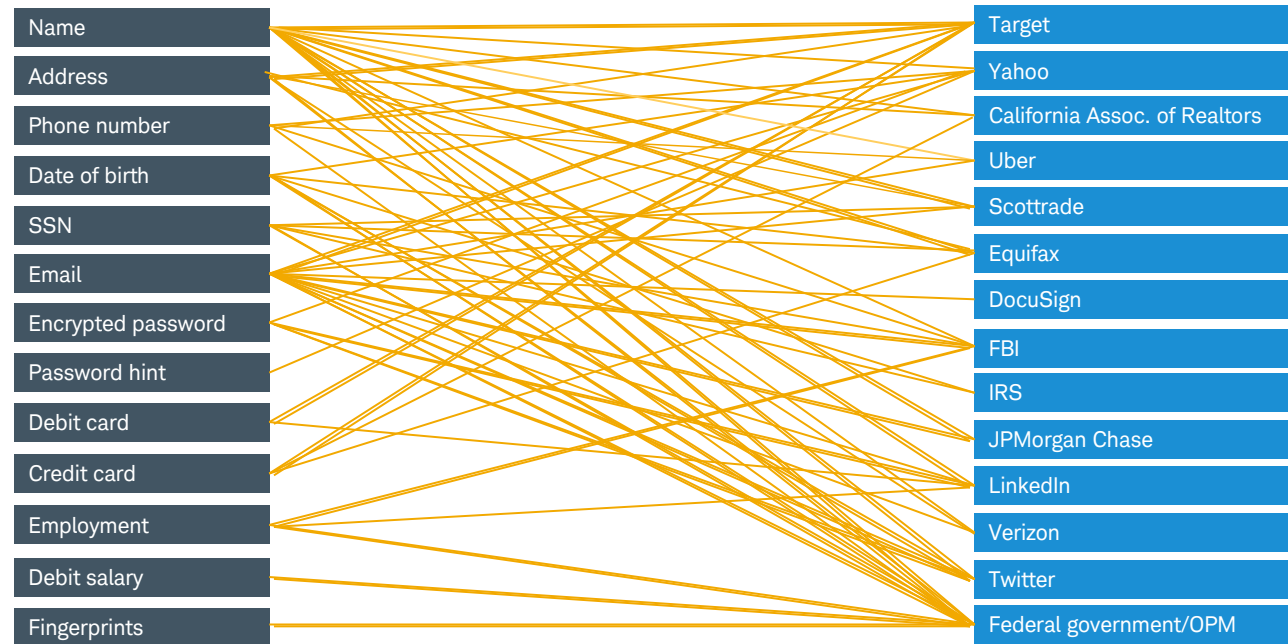
- Always use encryption to protect your information.
- Properly store your devices, keeping them inaccessible to criminals.

From a business perspective:

- Develop an effective cybersecurity program. See Schwab's [Cybersecurity Reference Guide](#) for additional information on strengthening your information security infrastructure.

Resource(s)

- [Data Breach Today](#)



4. Credential replay incident (CRI)

What is it?

Also known as credential stuffing, CRI occurs when login credentials obtained from an external source are tested in large numbers using automated login scripts against financial institutions' websites. The objective is to see if the credentials from the original site are the same as the ones used to log in to the financial institution's website. If a match is found, the fraudster now has access to the second account. Disbursements are then requested, or nonpublic information is acquired.

How does it happen?

Cybercriminals rely on human nature and our tendency to use the same username and passwords across sites. Passwords can be difficult to manage, so many consumers use the same login ID and password across multiple sites.

Often criminals obtain credentials in large numbers through a breach or from a list of previously stolen credentials being resold. They are then tested on other sites. While most of the credentials won't match an account, the law of averages works in their favor. By using a large cache of stolen credentials, they need to match less than 1% of the accounts to be successful.

Example(s)

ABC clothing company (company 1) is breached and 2 million client records are stolen, including user names and passwords to its online store. The credentials are tested in large numbers across various other sites. The perpetrator is successful in testing Joe Client's bank account, gaining access to his online bank account (company 2). The fraudster is now able to perform actions in Joe's bank account and initiates a wire transfer to South Africa.

Tips to prevent or identify

Encourage effective credential management techniques:

- Create strong and unique credentials for each site you access.
- Use a password manager.
- Employ two-layer authentication through a hard or soft token.
- Don't allow browsers to save or store passwords.
- Send information only through encrypted channels (HTTPS).

5. Account online compromise/takeover

What is it?

A fraudster gains unauthorized access to a client's existing online accounts, information, and assets via an online channel. Once entry into the account is made, unauthorized transactions such as trades and disbursements are initiated.

How does it happen?

Fraudsters acquire credentials from unauthorized sources and access the accounts using one of several methods. Some include:

- Credentials stolen through a data breach of either the business holding the account or another site
- Keylogging, phishing, malware, or other cyber techniques that can steal credentials
- Social engineering using partial client information to persuade an employee to reset credentials

Hackers may then change account information such as the email address or the phone number to circumvent discovery by the true end-client. Funds are then stolen through various disbursement channels. The prevalence of this type of fraud has increased along with the proliferation of data breaches.

Example(s)

The cybercriminal, Joe, performs Google and Facebook searches to obtain a few pieces of personal information about Steve, who has an account with ABC Financial. Joe then calls ABC Financial impersonating Steve and social-engineers the call rep to reset Steve's online password. Now able to access Steve's online account, Joe logs in, changes the email address and phone number, and then initiates several wire transfers out of the account and into a bank account under his control.

Tips to prevent or identify

- Employ safe use of software, activating firewalls and keeping systems updated.
- Enable browser security settings.
- Employ safe use of wireless networks.
- Practice effective password management such as password managers and dual-factor authentication.
- Educate yourself and others on top fraud trends.
- Be cautious with emails, including attachments and links from unknown sources.
- Monitor account activity regularly.
- **Enable two-factor authentication** for any website that provides this level of protection.

6. Distributed denial of service (DDoS) attack

What is it?

A server, website or other network is flooded with traffic created by cybercriminals, preventing legitimate users from accessing it and making service unavailable.

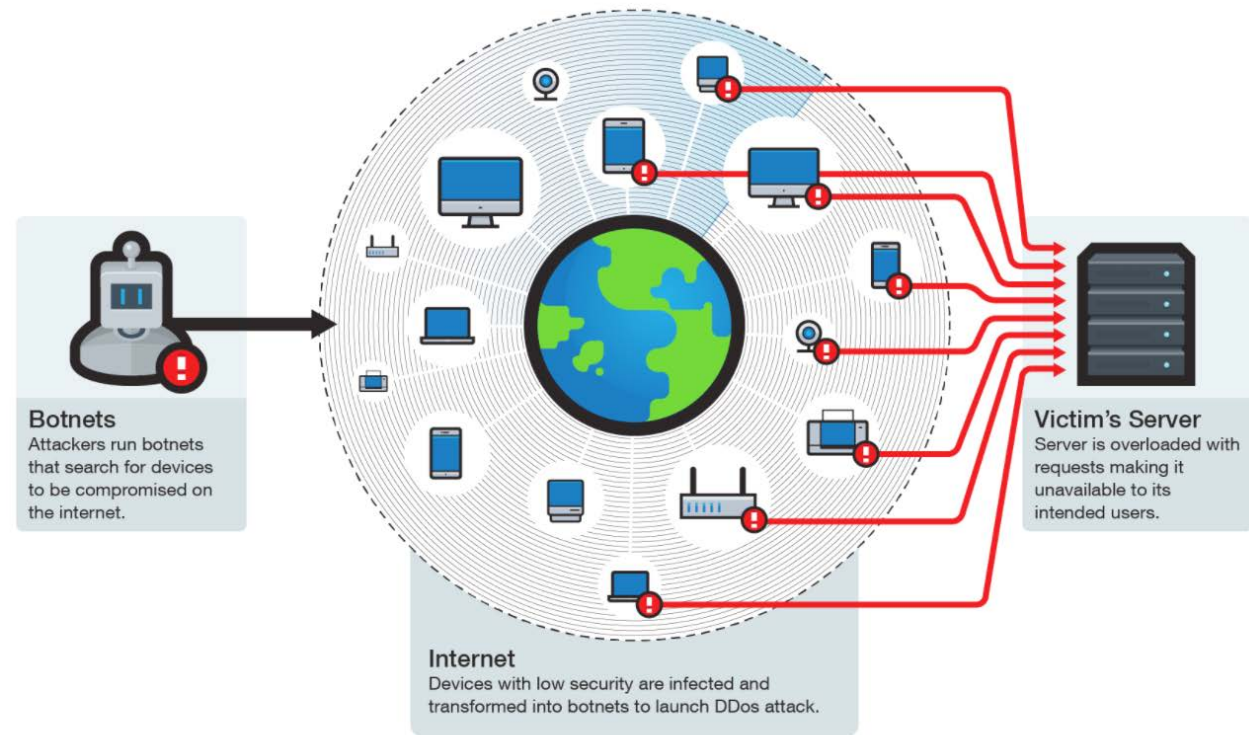
How does it happen?

Botnets, a network of Internet-connected devices under the control of a criminal, attack resources with overwhelming fake traffic to overload systems. The results are lowered performance, slowness, or complete disruption of the service for consumers. Hackers may use this attack vector for reasons such as extortion, malicious intent, bragging rights or gaming, distraction from other activities or attacks, business competition, and hacktivism (using the online channel to support a political agenda).

Example(s)

At right is a diagram of how a DDoS attack is perpetrated.

The Dyn cyberattack of October 2016 was the largest of its kind recorded, causing widespread Internet interruption in North America and Europe. The attack disrupted service to several popular websites such as CNN, Twitter, Netflix, and more. Setting a record at 1.2 terabytes per second, the devices used to perpetrate the incident included routers, webcams, smart TVs, DVRs, and more.



<http://blog.trendmicro.com/trendlabs-security-intelligence/internet-things-ecosystem-broken-fix/>

Tips to prevent or identify

- Employ firewalls and a block rule for detected IP addresses.
- Provide sufficient bandwidth for your services.
- Install cloud-based anti-DDoS services to detect and divert attacks.

Your fraud checklist

While fraudsters use a variety of techniques, a few consistent guiding principles can, if followed, help reduce your firm's overall fraud risk. You may use this checklist to supplement your internal controls.

Email scrutiny		
1.	Apply additional scrutiny when engaging in any email correspondence with a client, and always speak to your client before acting on emailed instructions.	<input type="checkbox"/>
2.	Ensure you are not providing additional information via email that could be beneficial to a fraudster.	<input type="checkbox"/>
3.	Look for use of frequently seen techniques such as sympathy, aggression, urgency, and inability to be contacted via phone.	<input type="checkbox"/>
4.	Pay closer attention to requests that inquire about differences between disbursement charges and fees.	<input type="checkbox"/>
5.	Inquire about emails sent with invoices or attachments that seem unnecessary for the request.	<input type="checkbox"/>
6.	Employ additional controls for verifying international wires, and ask your client detailed questions about the recipient.	<input type="checkbox"/>
7.	Look for language cues that deviate from English or your client's manner of speaking.	<input type="checkbox"/>
8.	Apply same controls to both first- and third-party requests.	<input type="checkbox"/>
9.	Employ controls within the firm for <i>internal</i> email disbursement requests.	<input type="checkbox"/>
10.	Employ customized controls such as fax coversheets or added documentation or signoff on emailed requests.	<input type="checkbox"/>

Verbally confirming client requests		
1.	Do not rely on the phone number used to call you as one of your authenticating tools.	<input type="checkbox"/>
2.	Casually present details you know about your client into the conversation to verify them.	<input type="checkbox"/>
3.	Go through all disbursement details, including recipient and account information.	<input type="checkbox"/>
4.	Ask questions about how the client received the instructions.	<input type="checkbox"/>
5.	Encourage clients to verbally verify transfer instructions with the recipient, and ask for supporting documentation if appropriate. An international wire, if deemed as fraud, is difficult recall.	<input type="checkbox"/>
6.	Assess the destination and whether it fits the client's pattern of behavior. Ask additional questions if the destination is atypical or it's the first time sending money to the recipient.	<input type="checkbox"/>
7.	Be on the lookout for scams, and inquire with the client if red flags are identified.	<input type="checkbox"/>
8.	Conduct online searches, check with the Better Business Bureau, and perform other due diligence in confirming the legitimacy of the offer or destination.	<input type="checkbox"/>

Safe cyber practices		
General		
1.	Educate yourself and others on top fraud trends. Understand the importance of cybersecurity, and the impact it can have on your firm's brand.	<input type="checkbox"/>
Malware/ransomware		
1.	Backup critical files and information regularly.	<input type="checkbox"/>
2.	Use multiple formats to store files, such as DVD, memory stick, or the cloud.	<input type="checkbox"/>
3.	Consider having a ransomware incident response and continuity plan.	<input type="checkbox"/>
4.	Implement a ransomware awareness and training program.	<input type="checkbox"/>
Software, OS, browser safety		
1.	Install antivirus and antispyware software on all platforms.	<input type="checkbox"/>
2.	Establish and maintain strong browser security settings.	<input type="checkbox"/>
3.	Keep web browsers and operating systems updated.	<input type="checkbox"/>
Password safety		
1.	Do not allow browsers to save passwords.	<input type="checkbox"/>
2.	Practice effective password management, such as using password managers and dual-factor authentication.	<input type="checkbox"/>
3.	Ensure passwords are strong and unique for each site.	<input type="checkbox"/>
Phishing		
1.	Be cautious with emails including attachments and links from unknown sources.	<input type="checkbox"/>
Wireless networks		
1.	Be aware of your surroundings when you work in public places.	<input type="checkbox"/>
2.	Remember to use encryption programs and to disable network applications whenever working in public.	<input type="checkbox"/>
3.	Pay attention to pop-up security networks.	<input type="checkbox"/>
4.	Disconnect any features that automatically connect you to outside networks as you travel.	<input type="checkbox"/>
5.	Avoid accessing public Wi-Fi, and use only wireless networks that are protected.	<input type="checkbox"/>
6.	If you cannot avoid using public Wi-Fi, do not accept software updates when connected.	<input type="checkbox"/>
7.	Install a virtual private network (VPN) or use a personal Wi-Fi hotspot for network access in public locations.	<input type="checkbox"/>

What to do if fraud is suspected		
1.	Report unauthorized transactions to Schwab, both successful and prevented events.	<input type="checkbox"/>
2.	Provide your clients with appropriate, immediate, and ongoing action steps. See the Cybersecurity Resource Center > How to Respond to a Data Breach flyer.	<input type="checkbox"/>
3.	Follow your internal escalation procedures.	<input type="checkbox"/>
4.	Remind your client of the Schwab Security Guarantee for safeguarding assets lost as a result of unauthorized transactions.	<input type="checkbox"/>
5.	Perform a post-event evaluation to assess your firm's process efficiency.	<input type="checkbox"/>
6.	Apply extra due diligence with future requests, and closely monitor client accounts for at least the next year.	<input type="checkbox"/>

Schwab Advisor Center[®] alerts

Your familiarity with your end-clients is one of the top lines of defense for preventing and detecting fraud. Alerts are tools Schwab uses to keep you in the loop regarding the activities being performed on behalf of your clients. These notifications can be a key risk-mitigation strategy for identifying behaviors that may fall outside expected parameters.

Alerts can be utilized to identify activities such as unauthorized trades, transfer of assets, and money movements. Certain activities such as contact information updates may signal a fraud event. Schwab also uses the alert system to notify you of other activities, such as unusual login behavior. Alerts that may indicate fraud include:

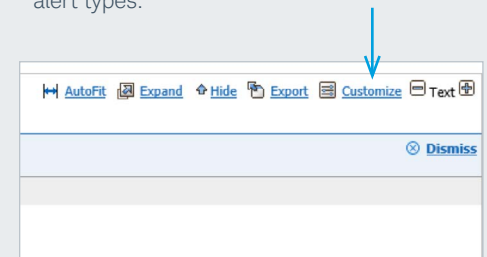
Alert type	Best practices
Account Change	Look for unusual or unanticipated updates to email addresses, physical addresses, or phone numbers, as criminals will often change contact information before performing a fraud event (e.g., a criminal will update a phone number before submitting wire instructions to circumvent verification calls).
Money Movement	Monitor for money movements that appear suspect. Pay close attention to wires, MoneyLink profile settings, and third-party checks.
Client Initiated	Money movements, trades, or email changes that are performed by the client will be sent under the Client Initiated alert type. Additional attention should be directed to these alerts to detect possible online account takeover on SchwabAlliance.com.
Transfer of Assets (TOA)	Be vigilant with alerts related to unfamiliar TOA requests, and contact your client to validate requests that were not anticipated, since fraud can occur in this channel.
Unusual Login Activity	Schwab will send alerts to notify you of some unusual login activities detected on your client's accounts. Look for notices, and work with your clients to take appropriate security actions.

Alert types to consider in helping mitigate fraud risk:

Alert types	On website	Via email
Account Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alternative Investments	<input type="checkbox"/>	<input type="checkbox"/>
AS Billing Team Notice	<input type="checkbox"/>	<input type="checkbox"/>
Client Initiated	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Corporate Action	<input type="checkbox"/>	<input type="checkbox"/>
Cost Basis	<input type="checkbox"/>	<input type="checkbox"/>
Cost Basis Team Notice	<input type="checkbox"/>	<input type="checkbox"/>
Dollar Cost Averaging	<input type="checkbox"/>	<input type="checkbox"/>
eSignature	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Accounts	<input type="checkbox"/>	<input type="checkbox"/>
Management Fees	<input type="checkbox"/>	<input type="checkbox"/>
Margins	<input type="checkbox"/>	<input type="checkbox"/>
Margins Team Notice	<input type="checkbox"/>	<input type="checkbox"/>
Money Movement	<input checked="" type="checkbox"/>	<input type="checkbox"/>
New Account	<input type="checkbox"/>	<input type="checkbox"/>
New Issues	<input type="checkbox"/>	<input type="checkbox"/>
Personal Trust Notice	<input type="checkbox"/>	<input type="checkbox"/>
Pledged Asset Line	<input type="checkbox"/>	<input type="checkbox"/>

See [Schwab Advisor Center®](#) for a current guide to using alerts and the types of alerts Schwab offers. We encourage you to establish your alerts filters properly so that you are receiving alerts that can be helpful in detecting and preventing fraud. From the Alerts page, you can access the Customize option and select the alerts you wish to see. Some of the alerts related to fraud activity are checked here.

Click **Customize** to pull up a menu of alert types:



Alert types to consider in helping mitigate fraud risk (continued):

Alert types	On website	Via email
Prime Broker	<input type="checkbox"/>	<input type="checkbox"/>
Report Available	<input type="checkbox"/>	<input type="checkbox"/>
Schwab Advisor Network	<input type="checkbox"/>	<input type="checkbox"/>
Service Requests	<input type="checkbox"/>	<input type="checkbox"/>
Service Team Notice	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Technology Scorecard	<input type="checkbox"/>	<input type="checkbox"/>
TradeAway	<input type="checkbox"/>	<input type="checkbox"/>
Trading	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Trading Team Notice	<input type="checkbox"/>	<input type="checkbox"/>
Transfer of Assets	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User	<input type="checkbox"/>	<input type="checkbox"/>
Wrap Fees/Adv Paid Fees	<input type="checkbox"/>	<input type="checkbox"/>

All rights reserved. Schwab Advisor Services™ serves independent investment advisors and includes the custody, trading, and support services of Schwab. Independent investment advisors are not owned by, affiliated with, or supervised by Schwab.

Neither Charles Schwab & Co. Inc. nor any of its affiliates or employees makes any warranty, express or implied, or assumes any liability or responsibility for the accuracy, completeness, regulatory compliance, or usefulness of any information, tools, resources, or process described in this *Fraud Encyclopedia*, or represents that its use would protect against fraud incidents, including but not limited to system breaches, compromise of firm security, and/or improper access to confidential information.

Neither Charles Schwab & Co., Inc. nor any of its affiliates or employees is responsible for any damages or other harm that might occur as a result of, or in spite of, use of any information, tools, resources, or processes described in this *Fraud Encyclopedia*. Your firm alone is responsible for securing your systems and data, including compliance with all applicable laws, regulations, and regulatory guidance.

References in the *Fraud Encyclopedia* to any specific product, process, or service by trade name, trademark, manufacturer, or otherwise do not necessarily constitute or imply its endorsement, recommendation, or favoring by Charles Schwab & Co. Inc. The *Fraud Encyclopedia* contains links to content that is available on third-party websites. Please note that Schwab does not endorse these sites or the information, products, and services you might find there.

Unless otherwise specified, examples and graphics are hypothetical and provided for illustrative purposes only.

For advisor use only. For general educational purposes.

Schwab does not provide legal, tax, or compliance advice. Consult professionals in these fields to address your specific circumstance.

©2018 Charles Schwab & Co., Inc. ("Schwab"). Member [SIPC](#).

AHA (0718-87E7) MKT97982WEB-01 (06/18)

00212175



Own your tomorrow.