23 January 2018

Financial Self-Defense: Preventing Fraud and Mischief

By Norb Vonnegut (https://blogs.cfainstitute.org/investor/author/norbvonnegut/) and L. Burke Files (https://blogs.cfainstitute.org/investor/author/lburkefiles/)

Posted In: Economics (https://blogs.cfainstitute.org/investor/category/economics/), History & Geopolitics (https://blogs.cfainstitute.org/investor/category/history-geopolitics/), Leadership, Management & Communication Skills (https://blogs.cfainstitute.org/investor/category/leadership-management-communication-skills/)

Got money?

You're a target for fraud.

Somebody once asked the famous thief Willie Sutton why he robbed banks.

"Because that's where the money is,"* he said. (https://quoteinvestigator.com/2013/02/10/where-money-is/#return-note-5417-1)

This irrefutable logic is telling because Sutton also targeted the homes of high-net-worth individuals. Posing as a delivery man for telegrams or flowers, he preyed on wealthy women, sometimes snatching jewelry worth hundreds of thousands of dollars from their homes in a single heist (https://www.amazon.com/Where-Money-Was-Memoirs-Robber/dp/067076115X).

Sutton was a meticulous thief who researched his targets obsessively. He knew their habits and schedules, knew when wealthy marks were about to attend major social events, knew when they had taken jewels from their safes. Until his capture in 1952

(http://www.nytimes.com/2002/02/17/nyregion/city-lore-willie-sutton-urbane-scoundrel.html), he set the gold standard for criminal research. And if Sutton were alive and active today, we have no doubt he would be a power user of the internet.

The resources available to thieves are infinite. The two of us have been trading stories about crook ingenuity for years, L. Burk Files as a private investigator, Norb Vonnegut as an author of financial thrillers. In this post, we discuss research (literally) about how criminals think, how they behave, and how you can spot their bad offerings. We also describe how they use the internet to do their jobs, and we hope our observations help you protect your clients from financial malfeasance.

Criminal Mindset, Criminal Behavior

Norb Vonnegut: Burke, you've been a financial investigator for 27 years. Do crooks have telltale personalities?

L. Burke Files: Sometimes. Anger, pride, power, suggestibility, and a loner mentality seem to be the most obvious characteristics, at least to me that is.

Take the first three. You can provoke *anger* quickly when you dare to question their ideas or background. You are injuring their *pride* and, perhaps, exposing their lack of expertise. Criminals typically respond with overwhelming force and *power* tactics. They threaten. They belittle. Or even better, they identify a common enemy: you or the "stupid adviser" who dared question them.

But anybody can pitch a fit. Happens all the time on Wall Street. How do you distinguish crooks from people with short fuses?

This is where *suggestibility* comes into play. You discuss a complicated situation with clear legal boundaries. Criminals exhibit a willingness to cross the line to get what they want.

But salespeople do the same thing, particularly in large organizations with complex rules. You know the old saying, "It's easier to ask forgiveness than it is to get permission."

It's a matter of degree. There is a difference between sales puffery and flat-out lying or producing fake financial documents. At some point, criminals break laws and violate ethics, and they always start with the little things to test boundaries and to see who may be watching. All schemes start small and grow.

What are the other clues?

Look at their lives. Crooks are single, or they partner up for only a few years at a time. The only exception I have ever seen is when both partners are criminals. As loners, they seldom share details about their work and personal lives. They are also overly sentimental about their pets and families, which is a technique for gaining acceptance and lowering your guard. Love a dog: You're okay. Kick a dog: You're a jerk.

Lack of empathy is another common trait. Some criminals respond to news stories about mass casualties by thinking: "I guess they got what they deserve," or "What a bunch of morons to lay down and take that." Of course, the most prevalent red flag is someone living beyond their means.

You steal it to spend it?

Right. Beyond the flashy restaurants, the expensive cars, the exotic vacations, the gaudy jewelry, and the over-the-top homes and offices, there is a link between the wheeler-dealer attitude and the criminal mind.

Clues to Bad Offerings

Norb Vonnegut: Background checks are one way to spot fraud. But how do you identify criminals from their sales pitches or offering documents?

L. Burke Files: I've seen plenty of fake documents, primarily from investors who hired me to recover funds they had already lost. In no special order, these are the indicators I see most often:

1. *Full-color brochures and highly styled pitch decks.* Graphics look good. But it's a problem if decks lack substance and somebody replies when you ask questions, "That information is confidential," or "I'll get back to you." It shows they are ignorant or lying — both red flags.

2. *Slipshod management histories in disclosure materials.* "She was a Senior Manager at an international company" could mean she was a greeter at IHOP or an underwriter at Lloyds. Who knows?

3. *Aversion to details.* All legitimate and successful executives respond to investor pushback with facts. They know their companies intimately. Crooks belittle the people who call them out. "Are you too stupid to understand?" They use arrogance and bluster to close the door to inquiry and hide their frauds.

4. *Clean desks, pristine office space.* These are showplaces, not work environments, how criminals envision the offices of, say, Hollywood moguls. A roomful of clutter is invariably where the real work and corporate growth take place.

5. *Implausible numbers.* A client asked me to evaluate bonds that were part of a $10-billion offering — two-year maturity, backed by diesel fuel from the Russian Republic of Bashkortostan. The figures were compiled by a Big 4 accounting firm in London (https://www.reuters.com/article/us-phantom-bond/special-report-the-bonds-that-turned-to-dust-idUSTRE77E1ST20110815). We checked with the firm and confirmed its favorable report. However, a quick back-of-the-envelope calculation showed that all Bashkortostan refineries could run 24 hours a day for three years and still not produce enough diesel fuel to collateralize the bonds. Our client avoided the deal, but several large European pension funds lost their entire investments.

6. *Guarantees offered in place of due diligence or assessment of the risk.* You hear this statement from time to time: "Our returns are guaranteed by (insert insurance product)." The offering might be legitimate, but the presence of third-party guarantees is always a starting whistle to dig into the reasons a company is willing to give up some of the profit of a product or project.

7. *Overly consistent returns.* The hockey stick that starts at the bottom left and rises at a 45-degree angle ever upward to the right, Excelsior!

8. *Pushy salespeople.* The trick is, isolate the victim and close the con before trusted advisers become part of the decision-making process. Criminals praise investors who agree with them and, conversely, belittle those who ask tough questions. They know second opinions could be their undoing.

9. *Absolute conviction.* When I hear, "Our projections are conservative," I usually ask two questions:

The first is: "What do you do if your expenses are too high or your sales are half your projections?" I am looking for a contrite acknowledgment from management that it is difficult to control costs, that assumptions are sometimes wrong. I want to hear insight, not arguments.

The other question is: "What happens if the projections are too conservative, and the company is growing twice as fast as you thought?"

If the promoter replies, "We have a party and celebrate," it's a problem. *Really? With investors' funds?* Meteoric growth will punish businesses unprepared for it. I want to hear management acknowledge the dangers and express their concerns.

10. *Complexity without economic purpose.* Offshore companies with trusts, foundations, IP banks, and other vehicles that complicate ownership are fine — if they serve an economic function.

How Criminals Use the Internet

Norb Vonnegut: What about Facebook, YouTube, Twitter, Reddit, Pinterest, Instagram, LinkedIn, and all the other usual suspects? How does social media put families in harm's way?

L. Burke Files: Too much disclosure about personal details and travel.

What I call "infoplague."

Right. A client challenged my point of view, saying it was too extreme. I offered to put her personal security to the test by evaluating her presence on social media.

Over the course of a few hours, I assembled her date of birth, complete background details on her brother and parents as well as her husband's parents. By the end of the day, I had the names of their banks and balance information for about half their accounts. It wasn't everything, but enough for crooks to empty their accounts, thanks to information posted by family members on social media.

Yikes. Is there an easy way for families to evaluate their risk?

Square the number of social media sites you use. It is four times more difficult to maintain a safe presence on two social media sites than one, nine times more difficult on three sites, and so on.

What are the "don'ts?"

No listing of births, deaths, parties, or names of your family members.

What can possibly go wrong from reporting the birth of a child or the death of a loved one?

The most valued ID to steal is that of a child as it will be years before anyone knows. The death of a loved one opens family members to inheritance scams as well as where the family gather might be of a wealthy family — such as the funeral services or gravesite service.

Uh-oh.

The second issue — travel — is even more serious. Your email autoresponder says, "I'm on vacation in Geneva." Now the crooks know your house is empty.

Even the most seemingly innocuous posts on social media can be dangerous — and photos are worth a thousand texts. There was a recent case involving two teenage siblings, members of a wealthy Swiss family. They posted a photo of themselves at their summer home in the South of France and reported that Mom and Dad would not arrive until several days later. *Home Alone* déjà vu. Kidnappers tried to take them in the middle of the night. Fortunately, security guards thwarted their efforts.

The data collection of our whereabouts is soaring. Facebook collects contacts from other apps and, using location-sharing data, knows when two friends are in the same place at the same time. Post on Pinterest, comment on Snapchat, use their software — and you can be located.

The issue goes beyond personal security. It extends to information that might aid your competitors. You might be negotiating a sale, round of funding, or launch of new product. Who you see and where you travel could reveal information that gives someone else a competitive advantage.

Technical Devices

Norb Vonnegut: So how do we manage our mobile devices? Without them, there would be no location data for social media to monitor.

L. Burke Files: Let's start with phones. Turn off location-sharing services when not in use. Apps like find my phone, find friends, and maps are terrific. But why send out data when they're not in use?

This is especially true of Wi-Fi and Bluetooth, which can communicate with any NFC (near field communication) cards and relay your card data over your phone to the fraudsters. Not only can the bad guys tell where you are, but they can take you on a spending spree you did not want. A bad guy with a Wi-Fi, Bluetooth, and NFC sniffer can steal almost all the information in your wallet and phone by just being near you as in, say, a mall or an airport.

When traveling, we suggest you leave cell phones at home and carry your documents and cards in a Wi-Fi- or radio-shielded wallet or purse.

Oh, come on. That's why we have cell phones.

For many you are correct. However, when we are talking about high-value targets — precautions are a must. They can forward calls from their normal cells to a service such as Kall8. Kall8 will forward calls to anyone you choose, even a foreign cell. Or just give out the Kall8 number, period. No one needs to know their cell numbers. Conversely, they can place calls from their cells through Kall8, and their cell numbers will not be shown to call recipients. There are other companies and more in-depth strategies — but this is a good start.

What about laptops?

Use virtual private networks (VPNs) when possible, search the web under the incognito or private modes of your web browser. Use browsers such as EPIC, Yandex, or Tor. Do not store passwords and information on the web or in your computer. If you have too many passwords, store them on an encrypted USB memory stick.

What about password managers. Why not use them?

It becomes a single point of weakness. While most are very secure, if the security is breached, the bad guys get everything.

What else?

Frankly, I recommend reserving one laptop just for international travel. It can be a "burner" or something new and powerful. The key is that it lacks all the digital data accumulated at home or at work. Keep critical documents on an encrypted USB memory stick, and when you return home, clean and reformat the machine. I recommend these extremes because other countries do not play by our rules. If you have traveled to China, Russia, or even France, your computer has been compromised and probably your cell phone, too.

Let's talk about home. I worry about security systems, cameras, and the internet of things, like Alexa or Siri.

You're right to worry. Put a Band-Aid on your computer's camera. Also, anything with an internet connection can get hacked. I'm including Wi-Fi-enabled devices such as doorbells, thermostats, even security cameras.

Security systems are a double-edged sword. If your security system is hack free, your information is private. But when criminals breach the perimeters, they can watch your most intimate comings and goings — like modern versions of Willie Sutton.

There is no way to be 100% safe. The idea is to make yourself a smaller, more difficult-to-reach target. Encourage criminals to look somewhere else.

If you liked this post, don't forget to subscribe to the *Enterprising Investor (http://blogs.cfainstitute.org/investor/follow-the-enterprising-investor/)*.

---

* Sutton denies saying it in his book *Where the Money Was (1976).*

All posts are the opinion of the author. As such, they should not be construed as investment advice, nor do the opinions expressed necessarily reflect the views of CFA Institute or the author's employer.

Images credit: ©Getty Images/CSA Images/Snapstock

Tags: cyber security (https://blogs.cfainstitute.org/investor/tag/cyber-security/), fraud (https://blogs.cfainstitute.org/investor/tag/fraud/), Investment Industry (https://blogs.cfainstitute.org/investor/tag/investment-industry/)

Share On

Facebook (https://www.facebook.com/sharer.php?u=http%3A%2F%2Fblogs.cfainstitute.org%2Finvestor%2F2018%2F02%2F12%2Ffinancial-defense-preventing-fraud-and-mischief%2F&t=Financial%20Defense%3A%20Preventing%20Fraud%20and%20Mischief) Twitter (https://twitter.com/intent/tweet?text=Financial%20Defense%3A%20Preventing%20Fraud%20and%20Mischief&url=http%3A%2F%2Fblogs.cfainstitute.org%2Finvestor%2F2018%2F02%2F12%2Ffinancial-defense-preventing-fraud-and-mischief%2F) LinkedIn (https://www.linkedin.com/shareArticle?mini=true&url=http%3A%2F%2Fblogs.cfainstitute.org%2Finvestor%2F2018%2F02%2F12%2Ffinancial-defense-preventing-fraud-and-mischief%2F&title=Financial%20Defense%3A%20Preventing%20Fraud%20and%20Mischief) E-Mail (mailto:?subject=Financial%20Defense%3A%20Preventing%20Fraud%20and%20Mischief&body=http%3A%2F%2Fblogs.cfainstitute.org%2Finvestor%2F2018%2F02%2F12%2Ffinancial-defense-preventing-fraud-and-mischief%2F)

About the Author(s)

Norb Vonnegut (https://blogs.cfainstitute.org/investor/author/norbvonnegut/)

Norb Vonnegut is a New York Times acclaimed novelist, who writes fiction and non-fiction about the financial services industry. Prior to his work as an author, he was a managing director with a registered investment adviser as well as an executive director at Morgan Stanley. Vonnegut is a graduate of Harvard College and Harvard Business School, and he believes that any day spent on the seat of a bicycle is a beautiful thing.

L. Burke Files (https://blogs.cfainstitute.org/investor/author/lburkefiles/)

L. Burke Files in an international financial investigator with three decades of experience. He is a specialist in international M&A and investment due diligence, with financial litigation support. Files has been the case manager on fraud

investigations ranging from thousands to over 20 billion dollars. He has run an investigation in over 130 countries. Files is a published author of several books, in particular, Due Diligence for the Financial Professional, which won two book awards.

1 thought on "Financial Self-Defense: Preventing Fraud and Mischief"

1. **— Anirudh says:**

   27 January 2018 at 20:01 (https://blogs.cfainstitute.org/investor/2018/01/23/financial-self-defense-preventing-fraud-and-mischief/#comment-540528)

   A real eye-opener for me.
   Thank you.

   Reply (/investor/2018/01/23/financial-self-defense-preventing-fraud-and-mischief/?replytocom=540528#respond)

Leave a Reply