Ep. 213 — Protecting What You Built: Liz Loewy on the Growing Threat of Elder Financial Fraud

The Patti Brennan Show — Full Transcript

This transcript has been edited for better readability. It has been lightly condensed and cleaned up for clarity while preserving the full content and meaning of the conversation.

Frank McAleer

Hello everyone, and welcome to The Patti Brennan Show. I'm your guest host for today, Frank McAleer. Whether you have $20 or $20 million, this show is here to help you protect, grow, and use your assets to build the best life possible. I joined Key earlier this year as Director of Longevity and Vitality Planning. Many of our clients listening know about our Vitality Hub — in essence, it's our effort to add resources to help you prepare not just for retirement, but for a better life overall. Key already does an excellent job of planning for our clients, but the Vitality Hub is about giving you additional resources, and I like to think of it like a diversified portfolio. We've vetted and researched resources for caregiving, aging in place, Medicare, choosing a home if you don't want to age in place, life organization, and — most importantly for today — fraud and theft protection. That's what today is all about, with our guest, Liz Loewy from EverSafe. In any portfolio, you want to manage your downside risk, and that's exactly what today is about: protecting you from fraud and theft.

Frank McAleer

Today isn't so much about how to use EverSafe — we recorded a webinar with Liz and her partner Howard last week that covers a full demo, and you can go back and watch that anytime. Today is about the "why" behind EverSafe: how the company was formed, what's happening out there with fraud and theft, and what we all need to be aware of to protect ourselves. Liz, thank you for making the trip.

Liz Loewy

My pleasure.

Frank McAleer

I think it's important for people to know why we chose EverSafe. First, you were the first mover in this space, as far as I can tell — some companies have since copied your model — but we chose you because of the passion you have for this work. So let's talk about how the business started. Liz, before EverSafe, you were with the Manhattan District Attorney's office, which is a pretty prestigious place to be. You started the elder abuse unit — what was the other unit you led before that?

Liz Loewy

I didn't lead it, but I oversaw domestic violence before moving to elder abuse and eventually starting the elder abuse unit. Like many prosecutors' offices, we had specialized units — domestic violence, child abuse, sex crimes, and others — but no unit focused specifically on older or vulnerable adults. Robert Morgenthau was the DA at the time. I asked him why we didn't have a unit focused on older and vulnerable people, and he said, "Go start it." So we did.

Frank McAleer

That was such a prestigious position. Why did you leave the DA's office to join Howard, your partner, who unfortunately couldn't be here today but is with us in spirit? Tell us that story — why you left and how you started this company.

Liz Loewy

Sure, that's a good question. Honestly, I never loved law school — I kind of hated it. Law had always been in the back of my mind as a possible career, but it didn't quite fit. I worked at a big firm at one point and didn't love that either, but then I interned at a DA's office and thought, "I could do this." Helping people, going to court — it was a great fit.

Frank McAleer

How many years were you there?

Liz Loewy

Over two decades. I started as a line assistant handling all types of cases, including homicides, then headed domestic violence before helping start the Elder Abuse Prosecution Unit — the first of its kind in the country, as far as we know. There should be more prosecutors' offices with dedicated units like that today, which is part of why we do the work we do now.

I had no plans to leave. I did that work for decades and really enjoyed it. But especially while running the elder abuse unit — I had about 18 prosecutors on the team — most of our cases involved older people who'd been defrauded or victimized. As a prosecutor, you get a little "twisted" in what you consider a great case: an older victim, a large amount of money stolen, a provable case, maybe even a confession. But it's genuinely very sad. You get the conviction, you put the person in jail, but the victims are left heartbroken — sometimes penniless. Their relatives have to take over, and it affects everyone: family caregivers, even the financial institutions involved, who feel they weren't able to do more.

I didn't plan to leave, but I met Howard Tischler. He called our unit during a case that had gotten some publicity, to talk about what happened to his mother — she'd been badly defrauded. After the trial, we talked, and he told me how he thought technology could help identify and shut down more of these cases.

Frank McAleer

And he's an experienced tech entrepreneur.

Liz Loewy

Very much so — though I didn't know that when he first called. Once I did, I thought: how great would it be to approach this from a different angle? Not just putting the bad guys in jail, but helping victims shut these cases down before the damage is done, and helping them get support if they've already been exploited. That's really how EverSafe started.

Frank McAleer

So even when you got a conviction, that didn't necessarily mean the money was recovered — is that what you're saying?

Liz Loewy

Right. Often the money's gone. People assume that because there's a trial, they'll get the money back, but many times the person who exploited them has already spent it, or you need a civil lawyer to try to recover it. Financial institutions usually aren't much help either — in many cases, their position is that if someone fell for a scam or allowed malware onto their computer, there's some contributory fault on the victim's part. It's awful.

Frank McAleer

That's a lot of what drives your passion, right? How do you get ahead of it and prevent the loss in the first place, since a conviction doesn't guarantee the money comes back? You mentioned a well-known case earlier — some of our listeners around our parents' age may remember Brooke Astor. Can you talk about that? It ties into something we'll get to: are wealthy individuals more susceptible to this kind of crime? I think the obvious answer is yes, but I'd love your take.

Liz Loewy

Well, where there's money, there are criminals who want it. It's the Willie Sutton logic — he robbed banks, and when asked why, he famously said, "That's where the money is." In this country, older people hold most of the wealth. There was an AARP-cited report — research from a few years back — showing the 50-plus generation held something like 82% of the wealth in this country. That figure may have shifted somewhat since, but the pattern holds: older people tend to be savers, generally speaking. I don't want to generalize too much or sound ageist, but older Americans hold a lot of wealth. At the same time, as we age we sometimes face challenges — memory issues, vision or hearing changes — and the Alzheimer's Association reports that one in three seniors dies with some form of dementia, most often Alzheimer's-related.

So when you think about "where the money is," plus older people living longer today than in the past — often with some of those challenges — that's a lot of money that isn't always well-guarded. I do think older, wealthy people may be disproportionately affected. But the statistics themselves aren't always precise. New York State cited a study by LifeSpan, based in Rochester, New York, that surveyed thousands of older adults and covered many aspects of elder fraud and financial abuse. One of the most cited statistics from that work: only 1 in 44 older adults report when they've been a victim of financial abuse. And that's just among people who could be interviewed — for those who couldn't, due to dementia or other reasons, it's likely even worse.

Frank McAleer

That's such an important number. We'll get into trusted advocates in a moment — but why do you think it goes unreported? Is it embarrassment?

Liz Loewy

If we're being candid, that study likely includes some incidents that weren't completed crimes — someone got a call, gave up a bit of personal information, but nothing more happened. To my knowledge, having been involved with that study, the figure wasn't strictly limited to fully investigated, founded crimes — but it's still a huge problem. Underreporting happens for a lot of reasons. One, as you said, is embarrassment — whether you're older or younger, if you've fallen for a scam, your first instinct usually isn't to call 911. Another is that these cases often involve family members. Most adult children are good people. But some come to believe their parents' money is essentially their own, and start making decisions before their parents actually need that kind of help. A power of attorney can be very useful, but it can also be misused — which brings us to the Astor case.

Brooke Astor — for those who don't know, the Astor family name is well known in New York City; there's an Astor Place subway stop, the Astoria neighborhood, and more — was defrauded not by a phone scammer, but by her own son. He worked for her, earned a good living managing her finances alongside some larger firms, and he was also her power of attorney, executor, and healthcare proxy. He was deeply trusted. When she developed what was believed to be Alzheimer's in her later years, around age 100, he began stealing from her with the help of an attorney. They were eventually prosecuted and convicted.

Frank McAleer

That's exactly why the concept of a trusted advocate matters so much. I'll jump ahead a bit — I'm an EverSafe client myself, and my wife and one of my daughters are my trusted advocates. Even when you trust someone completely, it seems like it still makes sense to have more than one, so there's more than one set of eyes. Can you explain what a trusted advocate actually is?

Liz Loewy

Sure. When I left the DA's office — and I felt very fortunate to have met Howard, who's had a long career in financial services and technology — we built EverSafe together. He asked me why these cases were so common even as crime overall was going down in New York, while elder financial abuse cases in my office kept rising. I told him three things.

First, scammers are very good at what they do, and they steal across multiple accounts rather than all at once. Even family members who steal — like Anthony Marshall, Brooke Astor's son — don't typically take a million dollars from one account in one shot. Scammers and thieves who want to avoid detection often start small and spread across accounts: checking, savings, then credit cards, investment accounts. But those accounts are siloed — there's no single view across them for most people. That's one reason people get away with it.

Second, even financial institutions that do monitor activity often aren't personalizing that monitoring to what's actually normal for you. You might gamble once a week — I know you don't, Frank — but if you did, we'd factor that into your baseline at EverSafe. We look at what's normal for each individual.

The third thing I told Howard — and I think the most important — is that people sometimes need help keeping an eye on all of their accounts: checking, savings, investment, retirement, four or five credit and debit cards. I told him it would help if we could monitor those accounts and also send alerts to trusted people. That's what we call "trusted advocates."

Frank McAleer

You call them trusted advocates —

Liz Loewy

Right, "trusted advocates." Regulators like FINRA use the term "trusted contact."

Frank McAleer

Got it, okay.

Liz Loewy

We had our own name for it first! We call them trusted advocates because they're advocating for you. They can't move money, and having one doesn't mean you're weak or "getting old." What I told Howard is that if account holders had a little extra support keeping an eye on things — not because they have dementia, but simply because they're busy, still working, traveling, living full lives — that would be valuable for anyone, older or younger. So we created a role: a designated person who can't move money, but who gets alerted to erratic activity. Howard said, "We can do that — we'll call them trusted advocates." That's part of why I'm so excited about the Vitality Hub — you all understand this.

Frank McAleer

That was a great answer, not too long at all. My trusted advocates haven't gotten many alerts, thankfully, since I haven't had much "malfeasance," for lack of a better word.

Liz Loewy

Maybe you need to start gambling once a week.

Frank McAleer

Buying AI stocks feels like gambling some days! But seriously, my trusted advocates don't get notified for every transaction — just anything out of the ordinary. And I love the algorithms behind the system. For listeners: EverSafe's algorithms learn your normal spending patterns. I'll get the occasional notice that I spent more than usual somewhere, and most of the time it's just because someone in my family spent more than normal. Can you talk about how those algorithms work? And also — since you mentioned accounts being siloed — one thing I love about EverSafe is that banking, investment, credit cards, trust accounts, and retirement accounts are all in one place. Nothing's siloed anymore.

Liz Loewy

Right. Both of those things matter. We look at spending categories — food spend is a good example, especially during the pandemic. If you were a trusted advocate for aging parents and their food spend went up a lot, that could mean they're simply eating more, or it could mean a caregiver has been hired and is spending on themselves too — what I used to call the "one for me, one for you" pattern, which I saw a lot as a prosecutor. We even had a case where that pattern eventually extended to buying a car for the caregiver. Categories matter in both directions — during COVID, we saw some older adults' food spending drop because they were afraid to go to the grocery store, which was also worth flagging to a trusted advocate.

Frank McAleer

So it's not every transaction — it's "maybe I should check in with my friend, my uncle, my aunt."

Liz Loewy

Exactly. And not every alert is about fraud or theft. It could be a missing regular deposit, like a pension check that didn't arrive — could be nothing, but worth knowing. It could be an unpaid bill, a bank error where an account was opened in your name without your knowledge, a scammer who's done the same thing, or a family member who's made an investment or wired money without your approval. Could be any number of things — but why not know about it? I don't know anyone who opens every bank, investment, and credit card statement the moment it arrives to compare them.

Frank McAleer

The envelopes just pile up.

Liz Loewy

Exactly — or they go unopened, and two months later you discover a wire transfer you never authorized. We also monitor real estate, since that's become a new frontier for scammers. And email.

Frank McAleer

I wanted to ask about real estate monitoring — I know from working with you there have been some fascinating cases. But first, for our listeners: I'm a client myself, and I get alerts on many of my transactions, which I appreciate — especially on my investment accounts, since I've been scammed before, and recovering from that is not fun.

Liz Loewy

It takes a while.

Frank McAleer

It really does. So — real estate monitoring. Tell us about that.

Liz Loewy

Sure. A lot of people have heard about real estate scams by now — scammers forging documents to make it look like a property has been sold, filing those papers with the county clerk, and the actual owner never finds out the title has changed.

Frank McAleer

The title has to formally change, and they're counting on the owner not knowing.

Liz Loewy

Exactly — and that's what we catch. Most counties don't notify homeowners in a timely way, if at all, when a title changes or a lien is filed. Some liens are legitimate — say, a contractor puts one on your property for a driveway repair and simply forgets to remove it once the work is paid off. Then years later you go to sell your house and discover a lien you didn't know about. We monitor for title changes, liens, and even reverse mortgage activity, along with bank statements. We had one case where a woman was in a medical facility for several months, and while she was away, people broke into her home, ransacked it, and forged paperwork to try to sell the house out from under her without her knowledge. We caught it and helped her attorneys shut it down — but that kind of thing can absolutely happen, and it's a mess to unwind.

Frank McAleer

Technology is helping scammers, but it's also helping you catch them.

Liz Loewy

Exactly — how could you not use technology at this point? I don't understand how people wouldn't use it to look beyond just one account. People often think, "My bank already sends me alerts." But your bank isn't looking at your 401(k) or your other credit cards — they're only seeing their own four walls. Scammers, on the other hand, are using every tool available to them. So you might as well fight fire with fire — you'll be far more likely to catch it and shut it down quickly.

Frank McAleer

Let's talk about some of the popular scams out there right now.

Liz Loewy

Sure — you and I have talked about a few of these.

Frank McAleer

One that got me was an invitation scam. It was sneaky, because it came from someone I actually knew — a friend I used to row with on Boathouse Row in Philadelphia.

Liz Loewy

I didn't know you rowed crew!

Frank McAleer

I did, back in the day.

Liz Loewy

I'm a Philly girl myself.

Frank McAleer

I know you are! Anyway — this friend had had a stroke, and the invite said there was a party being thrown for him at the boathouse. It seemed completely legitimate, and I love this guy, so I clicked into the invite. It asked me to sign into my Google account to view it, and — I was careless, honestly not sure what state of mind I was in — I did it.

Liz Loewy

If anyone ever asks you to do that, don't.

Frank McAleer

Lesson learned. Once they had access, they got into all my contacts, and everyone I know got a fake invite too. They're just trying to get into your system and find passwords. So — invitation scams, be careful out there.

Liz Loewy

And I don't mean to single out Evite, Paperless Post, or Punchbowl specifically — scammers count on the same psychology as the classic grandparent scam, which is still very common. With the invitation scam, the first thing to ask yourself is: is there really a party? Who's inviting me? What's the occasion? You're caught off guard either way — whether you're expecting an invite or not. And often the scammer picked up the connection from social media.

Frank McAleer

Oh my gosh, yes — people share so much.

Liz Loewy

People forget to keep their contacts and details private on social media. You can see where someone went to school, when they're on vacation, even the names of family members, since platforms like Meta have specific fields for that information. Invitation scams are a big one. So are text scams. And —

Frank McAleer

What about CAPTCHA scams?

Liz Loewy

Right, CAPTCHA — those little grids where you have to prove you're human by picking out every square with a traffic sign or a bus. People get so frustrated they just want to get through it. Some scammers have started using fake CAPTCHA prompts to get people to click certain things on their computer, which ends up installing malware. The FTC now recognizes this as a real scam pattern. CAPTCHA itself is legitimate and useful for companies verifying you're not a bot, but you should never follow instructions to hit a specific sequence of keys — that's more likely than not installing malware.

The E-ZPass text scam is still very popular too — we see several of those every week. People get a text about an E-ZPass bill, and whether or not they even use E-ZPass, it catches people off guard. Any imposter scam involving a government agency — the IRS, police, or your bank — is common too.

Frank McAleer
I laugh because I get those all the time.

Liz Loewy
The bank one is a big one. It usually starts with, "We're just confirming — is this Frank McAleer?"

Frank McAleer
Right, right —

Liz Loewy
Then they ask for your date of birth, and before you know it you're giving out information and only later realize you're not actually talking to your bank.

Frank McAleer
I got one that said my Social Security account had been hacked. I knew right away that didn't make sense — how do you hack a Social Security account?

Liz Loewy
Well, you're a bit more attuned to this because of the work you do with us. Scammers are genuinely very good at what they do.

Frank McAleer
That's exactly the point I wanted to make — people listening right now are thinking, "I'd never fall for that."

Liz Loewy
They're sophisticated.

Frank McAleer
Howard's used a term before — the "sucker list." Scammers essentially team up and share lists of people who seem susceptible. Is that connected to the dark web, or is that something separate?

Liz Loewy
It's different. I'm confident scammers do keep something like a "sucker list," though they may call it something else. The dark web is different — with how many data breaches have happened in this country, if you've ever used a credit card, I'd bet your information is out there somewhere for scammers to buy. A "sucker list" is more specific: names of people who've already fallen for a scam once, or who scammers know are vulnerable because they engaged with a call instead of hanging up. Howard's mother likely ended up on a list like that — she was in her 80s, legally blind, hadn't owned a car in years, and was sold an auto club membership because she kept saying "yes" to whoever called, even though the company itself was legitimate.

Frank McAleer
And she lost a significant amount of money — her life savings, from what you've told me.

Liz Loewy
Yes. After that first call, she started getting calls from other, less scrupulous businesses too. Eventually, Howard and his brothers hired someone to help her with bills — and that person ended up writing large checks to herself. This is a pattern with adult children and aging parents: if a parent seems to be doing okay, the "good" kids often hold back from asking too many questions, because they don't want to infantilize their parent or overstep. So they don't get involved until it's too late. With EverSafe, they can get alerts for unusual activity instead. Interestingly, it goes both ways too — we have older parents who've signed up as trusted advocates for their busy, traveling, middle-aged kids.

Frank McAleer
That's a great point.

Liz Loewy

Having a trusted advocate doesn't mean you're weak. No one can move money through EverSafe — but you can keep an eye on everything, including real estate and email, which we've added since those are common places scams start. You can't live a vital, good life if you've lost your life savings. It's heartbreaking, and it's genuinely hard to get any of it back.

Frank McAleer

Let's talk about the dark web for a second. Keep in mind, this core monitoring is included for clients through EverSafe. If you enroll, you'll likely get quite a few notices about the dark web at first, because EverSafe looks back historically to check for any suspicious activity that's already occurred.

Liz Loewy

Right, that's really about your credit file. When you enroll, we look back across all three credit bureaus —

Frank McAleer

All three, which I appreciate.

Liz Loewy

There are monitoring services out there that only look at one bureau. People assume, "I've already got one of those," but there are three bureaus, and an alert from one won't necessarily show up from another — which is why we monitor all three, and we send those alerts to your designated trusted advocate too. That's different from a lot of other services. Credit matters, but it's not everything — when I was a prosecutor, theft cases rarely started in someone's credit report, though they sometimes ended up there eventually. So we look at the underlying credit data, not just the report itself. And you mentioned you got a lot of alerts when you first signed up.

Frank McAleer

I did — dark web alerts. The good news is EverSafe doesn't just say "you're on the dark web" and leave it at that — it's worth calling and asking what it actually means. I've called the service team myself, 24/7, and they've always been friendly and knowledgeable. People should just understand what "the dark web" actually is when they sign up.

Liz Loewy

It's essentially where stolen data ends up after a breach — it gets sold there, and regular people like us can't access it.

Frank McAleer

Right, and there's not much you can do about the fact that it's out there — it's really just a signal to be extra careful.

Liz Loewy

We do give people specific guidance depending on what's exposed. If your name and a hashed email address are out there — meaning you can't see the whole thing — that calls for different advice than if your date of birth, Social Security number, and a credit card number are exposed. If you get a dark web alert at one in the morning, you don't have to wait until the next day — you can call us right then.

Frank McAleer

Good to know. One thing that really surprised me when you first explained it: a lot of people think a credit freeze is a cure-all once they've had a card compromised. But it's not, right?

Liz Loewy

Right. I have friends outside my professional life who'll get a letter in the mail — usually snail mail, not online — saying their data was exposed in a breach. They'll tell me, "I froze my credit, so I'm fine now." And the truth is, maybe that was the right move, or maybe the specific information exposed didn't require it — freezing your credit does tie things up a bit.

Frank McAleer

What exactly does freezing your credit do?

Liz Loewy

You're telling the credit bureaus not to allow new credit transactions based on your file while it's frozen — new loan or credit applications, essentially.

Frank McAleer

Got it — so it's not about using an existing credit card, it's about stopping new applications.

Liz Loewy

Right. There may be situations where using an existing card triggers an inquiry with the bureaus, but generally, freezing your credit is a smart step if it fits your situation — it just won't protect your financial accounts. Credit is a completely separate thing from your checking, savings, retirement, trust, or existing credit card accounts. Freezing your credit does nothing for those — which is part of why we built EverSafe, since scammers hit depository accounts just as often, if not more, than they show up on your credit. A classic example is tax refund fraud: someone files a tax return in your name, gets a refund, and that money goes into a depository account they've opened in your name. We specifically alert for newly opened depository accounts — a credit freeze wouldn't catch that at all. Another example: an old credit card sitting in a drawer that hasn't been used in months — if someone in your home takes it and uses it, a credit freeze won't stop that either. It won't stop someone from taking your debit card and PIN and withdrawing cash or making purchases. Freezing your credit is a good tool, but it's not a be-all, end-all solution, and I worry people think it is.

Frank McAleer

I remember a major credit bureau breach a number of years back — Equifax, I think?

Liz Loewy

Yes, Equifax — everyone talked about that one, and there have been several since.

Frank McAleer

I remember being an EverSafe client at the time, and you all sent out guidance on exactly what happened and what to do, which I really appreciated. What have we not covered today? Let me check my notes... I think we've hit almost everything. Anything we're missing?

Liz Loewy

I honestly don't think so. We covered trusted advocates, real estate, email, and all the account types we monitor.

Frank McAleer

We haven't really talked about how big this problem actually is.

Liz Loewy

Right — the latest figure, from the Consumer Federation of America, puts fraud losses at $119 billion in this country, affecting families broadly, not just older adults. That number was extrapolated from FBI data and accounts for the fact that so many cases go unreported — when a family member steals from you, you're generally not calling 911. Between family-related theft and outside scammers, the totals are enormous. But the good news is, people can genuinely do something to protect themselves. I wouldn't have left what I considered the best job in the world — prosecuting these cases — if I didn't believe that.

Frank McAleer

And I think it's a growing problem because technology keeps giving criminals better tools — they're always trying to stay one step ahead.

Liz Loewy

And more firms should be doing what you're doing here. You're a groundbreaker, Frank — I've thought that for a while.

Frank McAleer

I appreciate that — and so is Patti, with the Vitality Hub for our clients. Please check it out — it covers everything we've talked about today, plus caregiving, which is actually why I'm here.

Liz Loewy

Exactly, because you can actually do something about it — you can look at the technologies out there and encourage people to try them, even if they're initially resistant.

Frank McAleer

Our view is, people are going to use something like this anyway, so why not access it through us? It ties into everything we already do here, and we've thoroughly vetted and researched EverSafe — I know it inside and out at this point.

Liz Loewy

We've worked together for a couple of years now.

Frank McAleer

We have. So — sign up for EverSafe. I hope this conversation has made the case for why. There's really no reason not to. Decide who your trusted advocates will be. Any closing thoughts for our audience before we wrap up?

Liz Loewy

The one thing I'd leave people with is that most people assume this could never happen to them — or to a family member they're keeping an eye on. But almost every victim I've ever met felt exactly that way before it happened to them.

Frank McAleer

I'm a good example — between the fake invite and something that happened with my airline account...

Liz Loewy

The points issue, right?

Frank McAleer

Right — 71,000 points were taken, and we're still not sure if we can get them back. It happened because a scam site was set up to look almost identical to American Airlines' real domain, and I didn't catch it. So — double-check everything. Use email monitoring, real estate monitoring, all of it. You and Howard clearly have this covered, and I love how passionate you both are about it. No one should live a long, good life only to have this happen at the end of it.

Liz Loewy

It really is devastating.

Frank McAleer

Well, with that — thank you so much for making the trip, and for a great partnership. Thanks to Patti, and thanks to Evan for having us here live today. That's it for today's show, everyone — I hope you enjoyed it. This episode will be available on the Key Financial website if you want to revisit it or share it with someone. And don't forget about the webinar and the Vitality Hub, which go into more detail on how to sign up for and use EverSafe. Thanks again for being with us today, and thank you, Liz.

Liz Loewy

Thank you.