CUES 115: Fraud Prevention Is a Member Service—an Interview With Andy Shank

Electronic fraud is the 'bank robbery of the 21st century.'

Sponsored by Harland Clarke

Lisa Hochgraf 0:05
You're listening to The CUES Podcast, Episode 115.

Welcome to our latest show, CUES podcast listeners. Thank you for tuning in.

As you know, this podcast is where you can hear credit union industry leaders and cross-industry experts provide a wide range of perspectives on trends and topics relevant to you. My name is Lisa Hochgraf, senior editor for CUES and our *Credit Union Management* magazine.

Today's guest is Andy shank, VP of fraud and risk product management for CUES Supplier member Harland Clarke, the sponsor of this show.

Andy is passionate about fraud prevention and mitigation, a former state trooper and a former credit union, AVP of fraud and compliance, and he believes in helping people who have been scammed and also in bringing bad guys to justice.

In this show, Andy describes big-picture strategies credit unions can use to better prevent and mitigate fraud. He talks about how technology can aid credit unions in these efforts. Along the way, he tells some amazing stories. Be sure to listen all the way to the end to hear Andy tell about the most interesting fraud management experience he's had to date.

Okay, let's get started.

So, Andy, I've shared your bio with our listeners in the introduction to the show. And it's a particularly interesting one. To help our listeners get to know you a bit more, I wondered if you tell everyone what it was that got you interested in studying criminal justice and political science at American University?

Andy Shank 1:49
Well, it was definitely a strange path to get there. I ironically started out as a pre-med chemistry major at American. I was the kid in high school who took a lot of science classes and that just seemed like the appropriate path to go. But I hit the wall at organic chemistry, as many science majors can probably relate to. And I decided that chemistry and medicine were not my forte, after all. So, at American, they kind of have a general education program where you get to take a class from this section and a class from that section to sort of, you know, get you a broad foundation of classes, and I just stumbled into a class called Justice in America. And it was taught by a former MPD Officer of in DC, had lots of great stories about, you know, his police work and his time out on the streets. And I'd always been the kid who loved watching the show

COPS as a kid. And I just found myself, after that first class, kind of gravitating towards classes in that area.

So, it was by no grand design of my my life goal to become a criminal justice major, or a police officer, or whatever I've become today, it just kind of happened by happenstance. And when I finished college, you know, what do you do with a criminal justice degree really, I was looking for work.

I graduated in December of '99. And I had interned the previous summer at a consulting firm in Manhattan doing kind of tech relocations, for some of the big investment banks out there. So as you know, this is pre-9/11, as we'll get to in a moment, and you know, banks are taking over other banks and investment houses are taking over ones and our team was responsible for moving traders from their previous workspace to their new workspace. So if they were retained by the acquiring company, they'd leave their old work on Friday and be good to go on Monday with all the applications and trading platforms that they needed.

So I was commuting through the World Trade Center every morning. My home office for the consulting firm was actually on the 77th floor of One World Trade going on the path train into the bowels of the World Trade Center every morning. But being the kind of petulant 22-year-old I was, I kind of burnt out on the corporate grind after about a year. I was living in New Jersey, so I had an hour-and-a-half commute tacked on to either end of my workday, and the workdays were long. So I didn't love that after about a year.

So I started asking myself, "What do I What do I want to do? What's my real life goal? Or what's the path that I want to go on?" And I started looking at law enforcement, just thinking of my degree and thinking of, you know, watching COPS as a kid, and I tried to go the federal level first, but my eyesight wasn't good enough. You have to have pretty darn good uncorrected natural vision, which I didn't have LASIK at that point yet, so I was disqualified off the bat for that. And I just said, "What's the next, what's the next step?"

And I applied to the Indiana State Police and my parents were kind of aghast at first that their baby would get into such a dangerous line of work. But then, so I moved back home in January of 2001, started the police academy with the Indiana State Police in July of '01 and then 9/11 happened obviously in September.

So, you know, my old office building, you know, destroyed; some of the buildings I worked in, destroyed; and it kind of brought a new perspective to my newfound, dangerous line of work, that's even, even the seemingly safe corporate lines of work can have their moments. So my parents were I don't know if that made them more comfortable or just put it in a new perspective. But that's where the law enforcement started. And then my career has just kind of gone in it's very fun and unique path since then

Lisa Hochgraf 5:20

It's going to be fun to talk with you and learn more about it today. So, after you did your undergraduate work, you went on for a law degree at Indiana University. I'm curious. After your schooling and then now more than 20 years fighting the bad guys, I think is an okay way to put it, do you have a quote or a professional mantra that you live by that you'd be willing to share with our listeners?

Andy Shank 5:41
Absolutely. I would say that it's, it's largely related to just fighting tooth and nail for the most vulnerable amongst us, whether that's seniors and some of the fraud schemes that I saw at the credit union, and some of the fraud schemes that we see at Harland Clarke, or some of the cases that I worked at the FBI or with the state police, where you've got, you know, people who are being victimized due to English not being their primary language or they've got some disabilities of some sort. Those are the cases and the kind of stories from my past that really resonate with me still of really fighting, fighting for the people who can't fight back.

And, you know, we had lots of cases at the FBI and with the ISP where, you know, we'd have a rich investment victim who, you know, wasn't satisfied with the 8% that he was getting from the market. So he got conned by somebody saying, I'll give you a guarantee a 35% returns, and that guy's a victim, don't get me wrong, but he's not the kind of victim that loses everything. He might lose a half a million dollars, but he's still got $3 million left. So we would investigate the bad guy, we'd prosecute the bad guy, and you know, do whatever we needed to do for the victim. But I really just had a connection with the folks who did not assume any risk, the folks who, you know, maybe hired an attorney to help them with their personal injury claim, and that attorney ended up robbing them. So it was really the folks who either didn't see it coming, couldn't see it coming, and were really victimized and really kind of manipulated by the bad guys.

So, you know, that's one of the things that I would really, you know, kind of urge the listeners of this, in the credit union world is, you know, don't just look at fraud, as "This can hurt our own bottom line," like "This could be a risk to the credit union itself. You know, we might lose 10 grand on this, or five grand on this." Look at it as, "Our members might lose money here too," and treat that as they're trying to treat that as just as important as your own internal financial risks. Because if your member gets defrauded, and they're out of all of their money, and you allow it to happen, or you could have seen it happening and made maybe had a chance at stopping it, you know, you owe it to your members, it'll be looking out for them like that. So, you know, look at your members, see the activity going on in their accounts, and really, really fight for them if you feel like they're being victimized.

Lisa Hochgraf 7:51
What a wonderful call to action. We haven't highlighted your connection to credit unions. You worked at a credit union there in Indianapolis right.

Andy Shank 7:59

I did, I did. I worked at Elements Financial, which is the former Eli Lilly Federal Credit Union here in Indianapolis. And I love that organization. I still bank there. They are my primary financial institution with no intent of leaving. And I always give them a ton of credit for giving me the opportunity to jump from the public sector to the private sector. I was working for the state and saw a job vacancy at Elements that really interested me. It was the assistant vice president of fraud and investigations there. And I didn't think I had a chance in the world at it. I didn't have any private sector banking experience, since my you know, little foray back in 2000. And, you know, they gave me an interview. We talked about it. And I think they really valued that I was an outside set of eyes. I hadn't hadn't, I wouldn't say been corrupted, but I wasn't somebody who had been done nothing but banking their entire life. And I was able to kind of jump in feet first and look at things with a new perspective. It wasn't that, oh, this risk is a risk to Elements. I was like, "You know what, this is a member getting defrauded. And it may never cost elements a dime, but we owe it to them to really go help them if we can."

So it was a great kind of hybrid role for me. I still got to feel like a detective here in there; I still got to go knock on doors; I still got to help people. But it was also, you know, my intro to corporate America, essentially, and banking in general in the credit union world. So I'll always be very grateful to Lisa, Ron, Jeff and Chris and the folks over at Elements for for giving me that opportunity, one of the best spots of my entire career and always will be.

Lisa Hochgraf 9:36
I think that we share this love of credit unions. And I think that your perspective on the world seems to align well with credit unions since credit unions like to be people helping people, serve the underserved. So, this is lovely.

Talk to me sort of in general about how all of these experiences that you've had have come together now for your current role at Harland Clarke.

Andy Shank 9:58
Well, I think my time in law enforcement was very beneficial to empower me to kind of hit fraud head-on, you know, don't shy away from it. A lot of folks in the banking world kind of treat fraud as this, you know, scary little animal that we just try to shut in the closet and not talk about. But if you don't talk about it, and you don't approach it, and you don't, you know, really attack it head-on, you allow it to win.

So, at Elements that was, you know, having the kind of confidence to call up members just get on the phone and call people and say, "Hey, I know this isn't a fun conversation, but I really see some odd things going on on your account. And I'd love to talk to you about it." And you know, that is to me, to your point a moment ago, that's what credit unions bring to the banking space. They're not just numbers. These are members. These are family members of the credit union. And when I call those folks, and I tried to train some of my people to do it, as well. And it's, they're not fun conversations to have, because you're poking into somebody's private life of what they're doing. And they probably have a little internal red flag going off, a little alarm bell

going off in their head saying, “Maybe this is wrong, maybe I’m being defrauded,” but they’re clearly still doing it so that alarm bells not going off too loud.

But we always thought if we can call that person and show them the evidence, “Hey, you’ve never done this before. You’re sending wires to random countries. And that’s not that is a huge red flag, because look at this FBI article; look at this news article; you know, is there something you’d like to talk to us about?” I would say about half of the time, they would fess up and say, “You know, I met somebody online, and he’s gonna be my, say, you know, he’s my husband, and we’re going to get married.”

And we’d have to say, “I’m sorry to tell you this, but that’s not going to happen. And that money is probably long gone.” And then the other half of the time we maybe get hung up on. Maybe they would not listen to us at all, but at least we planted the seed that something might be going on that’s potentially criminal or that they’re being victimized. And a lot of times we would see that account behavior stop.

So they may not actually fess up on the phone or in person that they’re being defrauded. But you’d see the behavior stop. So, we were sometimes we looked at it that we were the straw that broke the camel’s back that kind of pushed them over the edge of, “Okay, if Andy at Elements thinks this is wrong, then maybe actually it is and I should look at what I’m doing, talk to a family member, phone a friend, you know.”

And that’s what I would tell people, “Do you have anybody in your household that you can talk to and run through this entire fact pattern, because some of the stories we would hear were so crazy that, you know, it started out as a surgery that I was going to get, and then it became an international adoption. And then they’re gonna bring a gold truck to my house, and I’m responsible for brokering this giant truck full of gold.”

And when the person says that story, tells you the story and how it all progressed, you want to just say, “Are you even hearing what you’re saying? Like, “Do you even hear the story you’re telling me?” I would always encourage them, “Go tell this to your husband. Go tell this to a friend and see what they do. And if they’re in arm’s reach, they’re probably going to grab me around the neck and take your take your online banking away.

But it was really just about letting them know that we cared about their financial wellness, their financial future. It wasn’t about Elements, protecting ourselves; it was about helping us protect them as a member. And at Harland Clarke, it’s kind of the same thing. But it’s on sort of a zoomed-out level. So, I talk to clients all the time. And that could be banks or credit unions, about you know, subject matter that’s way broader than just checks, which is, you know, what Harland Clarke is known for.

So, since I’ve lived the life at an FI, I can talk to them about AML monitoring and how to make themselves more secure, whether it’s new member onboarding, or new customer onboarding, which then kind of has a trickle-down effect that if you can clean up your customer base, then

your check program is more secure and more beneficial on every level. So, whether I knew it or not all, of my career steps were kind of building, building a foundation to where I am today.

Lisa Hochgraf 13:50
I love the reframing you've done for me of mitigating fraud of helping people avoid fraud. It's made me think while you were talking about collections, too, because that's a tough phone call, also. "Hey, you know, your payment's not here. What's going on? How can we help?" And those, those are service calls in a lot of ways. And it sounds to me like you've framed interactions with members about potential fraud in their accounts as a service call. "I'm here to help, you know, your financial situation, I want to make sure it's the best it can be for you." That's lovely.

Andy Shanks 14:22
Yeah. And there are surveys and studies out there that say, you know, digital detection of fraud on accounts is one of the bigger factors for acquisition and retention of customers. So, they may not appreciate it at the moment when you've told them that they're being defrauded, and that the money may be gone forever. But at the end of the day, they they will appreciate or at least they should appreciate the fact that their credit union was looking out for them and that they use they got that kind of personal attention to hopefully stop them from losing any more money.

Lisa Hochgraf 14:54
For sure. So let's jump into fraud more deeply. How would you define pay fraud, what exactly are we talking about?

Andy Shank 15:02
Well, I paint with a pretty broad brush here. I define that basically (as) anytime a bad guy electronically finds a way to move funds from point A to point B without authorization and without setting foot in a branch, for example. So, you know, it could be contact center fraud, you know, some social engineering, starting wire transfers, which, you know, we did see on occasion or attempts of that, on occasion, could be account takeover through online banking to initiate ACHs or wires or other digital payments, whether it's Venmo, or any of the other various services out there, could be card skimmers could be anything related to card fraud. Basically, it's i's the bank robbery of the 21st century.

You know, I look at some of the statistics on robberies, and I don't mean to diminish them at all, they are a sad fact of life, and they still do occur. But their instances are so far down over the last 10 years. And really, I attribute a lot of that to the kind of risk analysis by the bad guys. Why would you set foot in a branch with a gun and commit the most highly prosecuted crime in the nation when you can achieve the same ends by, you know, buying some credentials on the dark web or, you know, getting into somebody's online banking through social engineering to them or any other fraud schemes?

So it truly is the bank robbery of this century, you know, why take the risk of setting foot in a branch and risk the car chase afterwards when you can do everything from your from your smartphone, you know, 200 miles away, if not more?

Lisa Hochgraf 16:33
And what you're saying adds a whole new level of understanding for me about how the pandemic has impacted fraud, right, the cyber fraud has gone way up, right? Nobody wants to go anywhere in person.

Andy Shank 16:46
No, and it's, it's absolutely, you know, and we'll, we'll talk about it in a little bit, but the the the institutions listening need to take a step back and look at how they've approached the pandemic and what they've changed when it relates to remote working, transactional validation—and that's for their members and for their own internal processes, you know, sending wires out to vendors and ACHs to vendors and things like that. A lot of the processes that we kind of took for granted in the in-person days may need some freshening if you're working at least a hybrid remote type arrangement these days.

Lisa Hochgraf 17:19
Andy, you've touched on this a little bit now. But let's talk more deeply about what and who you find are impacted by payments fraud.

Andy Shank 17:28
But at the end of the day, we all are, you know, whether that's getting a notification that your debit or credit cards compromised and you've got to wait on a replacement. I mean, that's, that's more of an annoyance than it is a real impact. But you know, there's cost to your FI for that. You know, they may have fraud transactions that they have to eat there. They've got to pay for a new card. You've got to wait for a new card. You've got the inconvenience of transferring payments over. And you know, there are costs involved in all of that, that end up trickling down to the consumer. And that's in every level of commerce.

I mean, we all pay extra for groceries and retail items, and pretty much everything due to fraud, whether it's shoplifting or the interchange on a card transaction that's built in to counteract the fraud costs. You know, you don't need to be the victim of an account takeover situation to pay for fraud, like you're, we are all paying for it and in some way, shape or form. When it comes to credit unions, unfortunately, and not just credit unions, any any financial institution, the real sweet spot for bad guys, in my opinion, are the the kind of mid-sized financial institutions of this world. And those would be the institutions that are not so small that they know every member on a first-name basis, but not so huge, that they've got eight figures to throw at fraud mitigation every year.

So, it's that middle ground that really worries me. You know, the community bank, or the very small credit union, they've got their finger on the pulse of nearly everything going on under their roof. And then the giant bank on the other end of the spectrum, you know, they've got

internally created machine learning AI that spots bad stuff from a mile away. And then they've got the budget to absorb large fraud losses. But that middle pack, that giant area in the middle are the places that I think really need to put a lot of focus into that fraud mitigation and risk mitigation overall.

So, at the end of the day, everybody's impacted by it, whether it's higher prices, inconvenience, in even at the FI level, it's really about that middle ground where they need to … the second you start ignoring fraud mitigation, the second it's going to bite you.

Lisa Hochgraf 19:38
What are some of the common scams you're seeing today? And what would you suggest that credit unions do to try to combat those scams?

Unknown Speaker 19:47
Some most of the stuff that we see at Harland Clarke is is cyber-related. You know, we don't have a branch presence, we, you know, are operating through our financial institution clientele or a direct-to-consumer model. So, what we're seeing is kind of a garden variety ecommerce fraud. And that's a bad guy coming to us with a compromised checking account because they are trying to order checks on that account, and most likely a compromised or stolen credit card number as well.

So, we kind of have two levels, or two pieces of compromised data coming at us. And most of the transactions we've been able to pinpoint through some of our newer technology that most of the fraud that we experience originates overseas through some of the hotspot areas that are kind of stereotyped as being the hotspot fraud areas. You know, sometimes stereotypes end up being true and in this case, it is some of those, some of those locations that we sometimes make jokes about the fraud originating from. Sad but true, it is true for us.

And unfortunately, I know from my law enforcement days, when you know, fraud crosses a border, sometimes even a state border, it becomes very, very difficult to investigate and prosecute, and becomes even more difficult when it crosses an ocean. So you know, when we're talking about $100 fraud here, even if we have 1,000 of them, it's not going to get the FBI attention. You know, we you'd have to get up in the 7 million, you know, seven-figure incident per per loss or per loss per incident to even get some federal attention on something most of the time, and even even more, so if it's crossing an ocean.

So, we've kind of come to terms with the fact that most of our bad guys are nameless, faceless international folks, you know, working in a contact center somewhere—that prosecuting them or even referring them to law enforcement most of the time is kind of a fool's errand. You know, we always help law enforcement when requested, of course, but we we don't have aspirations that every every call is going to become a prosecution. And our situation is kind of unique in that, you know, we don't get all of the origin story details on fraud incidents, but from what I've see, a lot of it is elder fraud.

So, it's elder older folks getting victimized in some way, shape or form. And I never know from one instance to another what the actual entree for the bad guys was to to the victim. But the difficulty for us is, you know, if I call this victim up and say, "Hey Mr. Jones, I think you've been the victim of a fraud. You know, we have an order here that was placed through Harland Clarke that is in your name. You know, I'd like to talk to you about it," he probably thinks I'm a bad guy. He's never placed an order with Harland Clarke or he certainly hasn't recently, and he has no idea who I am, what I am, or whether I'm legitimate or not.

So, I would advise him myself to hang up on me and not give me any information. So, what we're working on is some new functionality here at Harland Clarke, where we can report that data back to our client FIs. So, we may get an order on Andy Shank's account at Elements that we spot as fraud because we know it was coming from a problem country or a problem geography or it's come from a repeat fraud offender to us.

Now if if—it's hard to use myself as both roles in this story here—but if Andy calls Andy and says, "Hey, we just got an order in your name at Harland Clarke," Victim Andy is gonna hang up on Harland Clarke Andy. But if we can get that information from Harland Clarke to the FI that holds that account, that FI is a known entity to the victim. So, they can call that person up and say, "Hey, Andy, this is the Projocta from Elements Financial, you know me because you know, we're a credit union and we all know each other, and we see some suspicious things on your account that did you place an order recently through Harland Clarke?" "No, I did not." "Okay. You may have an identity issue. It's time to get your accounts closed out, new account numbers issued. You know, let's take a look at your account relationship with us." And everybody wins.

At that point, Harland Clarke has provided our clients with a valuable tidbit of information. They're able to reach out to their members to say, "Hey, we've detected an issue." The credit union looks great. Harland Clarke looks great to the client. And we stopped a fraud, which is above and above all, the most important part

Lisa Hochgraf 24:00
It harkens back to your criminal justice studies, right?

Andy Shank 24:03
Yeah.

Lisa Hochgraf 24:04
When you when you actually get it all the way to "stop the fraud"?

Andy Shank 24:06
Yeah, well, I think that was one of the biggest adjustments of moving from law enforcement to the credit union is that there was some level of expected and almost accepted fraud. That was very hard for me to accept, and I still haven't accepted it to this to some level, you know, that it was like, "Oh, that was only 500 bucks," or "We're under budget for fraud for this quarter." And I just kind of it made me seethe, because my law enforcement roots said, "No, these are all bad

guys. And I want to go track them all down." And I had to kind of tone myself down because you've got to focus your attention here and there. But it really kind of just focused me that like, I need to investigate everything I possibly can. Because, you know, for every dollar that goes to a bad guy, it came out of somebody else's account, and that person is hurting because of that.

So you know, every credit union, every BSA officer, every fraud investigator at the credit unions, they they have a responsibility in my opinion to really attack these fraud incidents aggressively.

Lisa Hochgraf 25:02
We touched on this a little bit earlier when we were talking about the pandemic—and no one wanting to rob a bank because no one wanted to go to a bank for a while. But how would you say the pandemic in the bigger picture has impacted both trends in perpetrating fraud and trends in mitigating fraud?

Andy Shank 25:19
I'd say the No. 1 factor has been the transition from an in-person office environment to remote working. And that's, that's on several levels.

First there's there are extra barriers to validating things that, historically, you might have just walked down the hallway or popped your head, popped your head in your office, to your boss's office to say, "Hey, did you really want me to send this wire to the new account information at this new vendor," and your boss would say, "Wait a minute, I didn't send you that email," or, you know, "Let's check with somebody in finance before we do this" or whatever the case may be.

If part of your staff is working remote at this point, they may say, the "My my boss's bubble in Skype is red. They're in a meeting right now. I don't want to bother them," or "They're out of the office today," or "I don't know who to talk to you about this," you know, "It's just a small amount of money. I'm just gonna go ahead and send that payment to this new vendor."

So, it's really about processes and procedures changing because of the new remote or at least a hybrid work environment. So, you need to look at those kind of things that, you know, typically, you would say, "Go Go ask somebody before you send a payment over this dollar amount. Well, make sure that those policies and procedures are still strong, even with remote working. So, get those checks and balances in there, make sure that things are getting approved. And you know, I say it jokingly half the time to, you know, some of our contact center staff here, is I don't want people having to make tough decisions, like your policies and procedures should write out or give them the guidance they need, that the policy and the procedure makes the decision, not the individual.

Because if you start making folks that are not in management level, who aren't being compensated to make very heavy decisions, you start expecting them to make decisions, everything else is going to start crumbling down because it's not fair to them. So, your policies

and procedures need to dictate most decisions. And when it doesn't, that's when the procedure to validate things needs to come into play. So, it needs to be very, very stipulated over X dollars needs this level of approval. And we check it on this level, that level. And that's even more important these days with the remote working environment.

The next level would be, were your IT systems designed for remote working. You know, when everybody was in the office, perhaps you didn't need multi-factor authentication because your system would only allow you to log in from the computer that's physically on your desk or in your office. But if you've changed, like we've all changed where you know, you may be doing hybrid or as everybody's remote, did your access systems.

So, your access security to your systems change with the times. So, you know, we it might be extraneous or too much to require that MFA when you're in an office in an in-office environment. But having that when somebody is remote can be a different a big game-changer.

So, you know, that push message that you get to your phone that says are you trying to log in and you click, "Yes," might be too much in the office. But when you're when your employees are sitting at home on their their sofa, like I'm doing right now, that extra message keeps the bad guy out. Because you have to ask yourself, "What could a bad guy do if he got my username and password?"

Okay, so if you're if you're systems are secure, and someone gets a username and password of a user, there's very little they can do to get in and do damage with just that username and password. Because I'm going to get a push message or I'm going to get some other level of additional validation that only I can do via my phone or via however you structure it. If you ask yourself, "If a bad guy got a username and password of one of my employees, what could they do?" and the answer isn't good, then you need to assess that.

And even then, once somebody gets in, you need to make sure that they only have access and authority to the systems and processes that they actually need. So, does every employee, including your summer intern, need transactional access in your core system? Probably not. So that should be something, pandemic or not. That's your IT and compliance teams are looking at on a periodic basis, making sure only the people who need it have the most sensitive access to your systems.

Lisa Hochgraf 29:25
So, controls sound like a great tool for helping to prevent fraud or to manage fraud. What would you say are the top three when you think about recommending ways that credit unions can mitigate fraud or prevent fraud? What would you talk to them about?

Andy Shank 29:40
Well, I would say that they don't want to focus too much in any one area because if you put all your eggs in one basket, then the other two of our three are going to be neglected. So, you need to create a holistic and kind of well-rounded approach to security and fraud.

The first piece of that foundation, I would say is that secure IT infrastructure. Make sure, and that's not just login and password type stuff, but make sure your systems are very difficult to penetrate via traditional hacking. Make sure that you've got folks monitoring your network to make sure there are no intrusions. And also, you know, know your limitations. You shouldn't rely on your internal IT security guy to handle everything. There are professionals in this world who can look at it and they do this as their full-time job day in and day out, to look to look at networks and say, "Yes, you're secure. No, you're not." Let's make these changes. Let's make sure this patch is done; make sure all your systems are updated. You know, we're all very good at our own job responsibilities, but you have to, you have to acknowledge your own limitations. So spend a little money to make sure your systems are robust and secure in it pays for itself via the the inherent security, the obvious, you know, we're hard to hack. But it also pays for itself when the regulators come in, when the NCUA comes in. And via your own peace of mind.

I mean, if you get one breach or one hack, I mean, that could put your entire institution out of business. So, it really makes you know, spending 50, 75 grand a year whatever that terrible-to-stomach-cost is, it doesn't sound so bad when the alternative is a bad guy gets in and now we're out of business.

The second kind of plank of this, I would say, is new account onboarding. So, you've kind of created your strong wall around, that's your IT security, your infrastructure is strong. And then you need to worry about how do we take in new members? And how do we validate those new members that they truly are who they say they are, and that they truly are someone that we want to do business with. It's a lot harder for bad guy to steal from you if you've never even let him in the door. And, in this day and age, you have to think a little more up-to-date or a little more technological than the the kind of credit report-based validation that we all have been relying on for far too long. You know, asking somebody you what street did you live on in Cleveland in 1998, those kind of credit report-based questions. To me, those are completely outmoded, and completely ineffective these days.

And after some of the big breaches of the last couple of years, that kind of information is just too out there. Every guy on the dark web is buying credit reports left and right. I mean, they are out there. And I always use the mental image of a bad guy sitting at a desk with a stack of credit reports in front of him. I mean, literally a paper stack. And this is just my mental image. But and I always ask myself, "Could someone open an account at Elements with a credit report of a victim in front of them? And if the answer is yes, then you need to tighten up the tighten up the gates.

So, when you ask him that question of, okay, who holds your car loan and you think you're being sneaky? Instead of him walking away, he just flips to page six, and he finds out who holds that car loan. So, if you're going to ask questions like that, and they still do have some value, but you have to add a secondary level of difficulty to it. Like you have to put a timer on that question. Like if you allow him unlimited time to go research that, he's gonna find the answer. But if you say, who currently holds your car loan, and you've got a timer with 10, 9, 8, 7, 6, 5, 4

going down, that's a little tougher to find, because you may not be that ready with it. I would still advocate for more up-to-date and more beneficial processes than just those credit report-based kind of validation on the front end. But if you're gonna have them, they'd better be sharpened.

You know, at Harland Clarke, we've jumped pretty, pretty hard into device-level technology for transactional validation. So that's beyond is this Andy on the other end of the transaction, it's it does that as well, but it's also has this device has Andy's iPhone, or has Andy's iPad become a problem anywhere else? And that's, that's really what it comes down to is information-sharing between merchants in between, you know, those who are the vehicles for the fraud. You know, we're able to tap into a world that's much larger than our own. We're kind of unique in our presence. So, you know, we may only see our customers every 18 months, or however long the gap is when they need checks or supplies from us. So, we don't have the benefits of an Amazon or a Netflix where they're seeing their customers two to three times a week. And a lot can change in the gap between when we saw the customer last and when we're seeing them now. So, you might have moved; you might have gotten a new phone, a new job. So, therefore, your email's changed; a lot of things can change. So, if we're relying purely on our historical order history, we're outdated at that point because things have changed. You may want to update addresses, and if we don't allow you to do that, then we lose. We lose a sale; we lose a customer.

So, what we've looked at and what we've implemented is a device-level vendor that allows us to tap into every client to this vendor to say, "Okay, that phone that Andy is on, that has been seen on 10 other transactions in the last 30 days and they're using the same address as Andy. They're using the same email address, the IP address. All four IP addresses that we pull are geographically appropriate for where Andy claims to be. This is a low-risk transaction. So, we should allow that.

On the other end of the spectrum, if somebody is trying to place order, orders in Andy's name, and that same device or that same IP number, or same IP address or same, any other attribute of that device or that person has defrauded another member of the consortium, that's going to come in as a much higher risk transaction. And we either have the opportunity to completely block it or route it to a review queue so we can look at it on a one-to-one basis. So it's a it's it's a lot about just making sure that your onboarding and your validation of who's on the other end of that now-remote transaction is who they say they are and it's somebody that you want to do business with.

The third plank of that, I would say is, you know, we've secured the it, we've fixed your gates, where you're letting in new members, you now you've got members in that are hopefully, you know, almost by and large, entirely the folks that you want, but what are you doing to monitor them once they're in. So looking at your members transactions for anomalous activity. Ao and that could be a member going bad, that could be somebody that snuck in and is now being a problem through remote deposit or payments fraud of any sort. Or that could be somebody who's being victimized in a fraud scheme.

So, make sure that your AML system or whatever system that you designate for your transactional monitoring is up to speed. And you've got processes in place behind that. So when that system says "Alert, Andy just took out $800 in cash and he never does that," make sure you know what to do with that, you know, put them on a review list, put them on a higher risk population within your AML software to say, "Okay, we're going to take another look at him in a week, and make sure everything's okay." And again, I always harken back to it, you'll never remove the human element from fraud detection, you can get all the technology in the world. But at the end of the day, there's no replacement for picking up that phone and calling me up and saying, "Andy, you just took 800 bucks out is is that normal? We don't see that, you know, we know it's not normal. But is everything okay?" And if I say, "Yeah, I just needed to go buy a new lawnmower or something and the guy only takes cash," case closed. Now, you've also you figured that instance out, and you've got a story to back it up. But if I take 800 bucks out the following Thursday, as well, it's kind of unbelievable that I would now need a second lawnmower. So, you've got to document that information as well, because that could theoretically turn into a SAR. If Andy claims he's buying a new lawnmower every Thursday, and I'm not operating a lawn care business, you, by definition, have suspicious activity.

So, it's all about protecting your members protecting the institution. And you know, getting the documents in the the proper evidence you need for SAR filings to law enforcement or wherever it may lead. So it's it's a lot to take in I know. But you're you're really doing your members and society a good service when you take this stuff seriously.

Lisa Hochgraf 37:45
For sure.

Andy, I'm wondering if you can tell me more about the spectrum of what's available in security technology today? What's the range of capabilities for credit unions using this tech?

Andy Shank 37:57
Well, the sky is really the limit. I mean, there are vendors that will sell you anything you want to pay for basically and you really just have to ask yourself, you know, "What is our risk and what is our appetite for that risk?" At Elements, we didn't have a huge branch presence and the branches that we had were behind security at corporate facilities for the most part. So, our risk was kind of different than an institution that has, you know, branches all over town and a drive-up window, and you're worried about the felony lane gang, and all that stuff. So, we were able to kind of focus our attention on the payments, fraud angle, the new account acquisition, and things like that.

So, you really just have to look at your own specific footprint of where your risk lies. And this isn't just about how much money can we stomach losing as a direct loss from fraud incidents? You have to think of it from a larger perspective than that it's reputational cost, its regulatory scrutiny. And then last but probably least the direct cost of fraud.

So, my guidance would be not to look at fraud and risk mitigation as purely a black hole of sunk costs. This is actually money well spent. So you know, we mentioned in a moment ago, one breach could put you out of business. So it's not so crazy to spend 75K a year on network monitoring when you look at it that way.

And, you know, don't look at your fraud mitigation as purely friction as well. That's a lot of the pushback that I've gotten in the past is, "Well, we don't want to you know, put this protocol in because it's, you know, it might make a good member say, 'I don't want to go through this process. I don't want to do that.'"

But there's a flip side to fraud mitigation, that it doesn't just stop the bad guys, but it can actually when, when properly tuned, it can actually make the experience for good guys smoother. So, if I can say this is the same device that Andy's always come in on. He's geographically appropriate for where he normally is. I don't need to ask him all those questions this time. So, your fraud mitigation software can it's a double-edged sword in a good way. It stops the bad guys and it helps the good guys get through with less friction than they would be without it.

And we said it a moment ago, but don't always rely just on tech solutions. There always be a human element in security and fraud mitigation. And it's beyond just empowering your staff to contact members or make the phone calls when you think something's amiss. You know, band together with other credit unions and other FIs in your area. Here in Indianapolis, we had a very good and strong fraud working group with some of the local police departments and a lot of the BSA officers and fraud investigators from the local credit unions and kind of mid-size banks around here. One of the things I love about the credit union ecosystem is that, you know, while we're all theoretically competing for members and business, when it came to fraud, it was it was all-hands-on-deck collaboration. So you know, no one wins when the bad guys wins. So there was I don't recall ever calling a credit union and saying, "Hey, you know, I've got some money laundering concerns with this member, and I see that you they may have a relationship with you guys, can we talk to see if there's risk here?" I don't ever remember a credit union saying, "Nope, we have no interest in talking to you about this." So it was it was wonderful. I, I hated to see fraud. But when I saw fraud, and it was a credit union on the other end, I was like, "Yes, I may actually get somewhere here."

So, you know, work together with your, your friendly competitors—and that's trends, suspects methods. And, you know, even even the government recognizes the benefit of information-sharing these days, you know. There there are specific sections in the BSA code that not only allow sharing of information, but actually encourage it. So, you know, look for those, get with your legal counsel. I think the code says, you know, something about if you can, you can articulate that it's terrorist financing or money laundering, you have the ability and the encouragement of the government to share information.

Now, money laundering is a pretty broad and vague definition. But we defined it pretty broadly that anytime you're trying to conceal the funds of an illicit act, that essentially is money

laundering. So, we would use that framework to contact other FIs and say, “Hey, we’re contacting you via this section of the BSA. We’d like to know about this member, this customer of yours. Let’s talk.” And if they did, the whole purpose was we would both construct a better SAR, and then that better SAR gets to law enforcement. And if there’s something truly criminal going on, then that SAR is much more actionable than a poorly written SAR without those details. And I’ve been on the receiving and the production end of SARS and, I’ll tell you, there are a lot of bad ones out there where people are literally just going through the motions. This person came in and cashed a check that we believe was fraudulent. Done. That’s it. But if you write a really good SAR, this person came in on this date with check number this with from account number this at this bank, and they were driving this car and doing this, that is a SAR that will rise to the top of the pack. And I know SARS aren’t a competition, but the goal is to make actionable SARS for law enforcement. And one of the best ways to do that is through that collaboration that’s actually encouraged through the BSA.

Lisa Hochgraf 43:17
I think there's a whole nother article in how to create a SAR that will get really good points and rise to the top.

Andy Shank 43:24
Well, and it's it's it's kind of a crazy self-fulfilling prophecy because a lot of BSA officers in banking, they they look at SARS as just kind of going through the motions, and they have this vision that is sometimes true that every SAR they they file just falls into a black hole of the government, is never looked at, is never investigated, is never acknowledged and the self-fulfilling prophecy is the reason that there are so many stars that fall into that black hole is the regulators have encouraged that you have to file a SAR on this, you have to file a SAR on that. And then it almost creates an environment where a high proportion of SARS are are junk because they are required and aren't necessarily full of actionable content.

So my goal was always you know, we're gonna file every SAR we have to file, of course. But we're not just going to go through the motions on them, we're going to get every piece of data we can. Of that check that we thought was suspicious went to a different financial institution, we're going to contact them and say, “What can you tell us?” And if the answer's nothing, they're not going to tell us anything, we're right back where we started. But if they gave us something, then it was better than where we were. So, you know, we write better SARS than they will be more actionable. And you'll have more faith in the process, because you'll start getting those calls from law enforcement saying, “Hey, I want the supporting docs on that one.” And that's the real badge of honor of a SAR is when you say, “Oh my gosh, somebody actually read it, and now they want to react to it.” So, but it all starts with writing better ones and making sure you get all the information you can.

Lisa Hochgraf 44:36
And just in case we didn't say full out what SAR is … SAR stands for…

Andy Shank 44:41

Suspicious Activity Report

Lisa Hochgraf 44:43
Right? I think most people will probably know, but just in case ..

Andy Shank 44:47
It depends on the audience. But it's a great point. I mean, there are there are lots of guidance in the code about when a SAR must be written: dollar amount, if you can't identify a subject, and then a much lower dollar amount if you can identify a suspect. So, I've been out of the game for a couple years now in my SAR-writing function. So, I don't want to quote too many rules on when or when they shouldn't be written. But those who know, know, and just know that, you know, there are people on the back end looking at those, you know.

When I was at the FBI, you know, we had analysts that would filter on specific terms. They had, you know, geography set out and if it involved public corruption, because you know, all those checkboxes on the SAR where you can say this one is, you know, money laundering or this one's public corruption or bribes and kickbacks. There are processes out there that are looking at those. So, write better SARS, and you'll get better reactions. That's really where it's at.

Lisa Hochgraf 45:38
Andy, this has been a lot of really great information for credit unions to consider. Before we wrap up, I want to ask you a closing question just for fun. Would you tell our listeners in the CUES Podcast nation about the most interesting fraud scheme you've seen at a financial institution and what the financial institution was able to do about it?

Andy Shank 45:57
Sure. And ironically, this one's not particularly crafty. It's not super ingenious or anything like that. It's kind of a, again, a garden-variety fraud scheme. But it's got a lot of twists and turns to it.

So I was at Elements. And I've been there about four months. And you know, this kind of gets back to my passion of like helping the most vulnerable people and really kind of putting that extra effort in for the folks who are clearly being victimized. And, you know, we saw the full spectrum of fraud, whether it was romance fraud, foreign lottery schemes, Craigslist, work from home, all of, all of those kind of things. But there is certainly one incident that sticks out to me,

We had an older member. He was a retiree, a very, very intelligent man. I think he even had a Ph.D. He was an assisted living home. And he actually got a postcard in the mail. And it basically just asked him if he wanted to enter a foreign lottery, like an international lottery, and it just required a checkbox from him. It was all bar coded and pre-stamped for the return. And so, he checked, sure, who wouldn't want to enter a foreign lottery scheme with a free, postage-paid postcard to drop it back in.

So just pausing there, that alone shows you the sophistication of the crews that are pulling these schemes, you know. This isn't a kid in his mom's basement who's just figured out try to defraud some people. This is a legitimate criminal organization. So, they have a marketing department. They're using direct mail. They know to paper retirement homes, who are their kind of chosen victims with these postcards. And the crazy part about these fraud schemes is there's no, there's no penalty for failure for these bad guys. You know, they might spend 1,000 bucks on paper and postage for these postcards. But if one of them pays off, then they're money ahead.

So, you know, he sends the payment that postcard back in and he starts getting calls, saying that he'd won second prize. They didn't oversell it and say that he had won the million-dollar grand prize, but he'd won the half a million dollars second prize. And, you know, we all know where this is going with these fraud schemes. He has to pre-pay the taxes ahead of time.

So, all of this occurred before anybody at Elements was aware of anything and the way that we found out was some of our awesome branch staff at a at a branch. He was a familiar customer to them, and he would come in and he was not a cash-intensive member by any stretch. But all the out of the blue, he starts coming in and he wants 1,000 cash every single day, Monday, Tuesday, Wednesday, Thursday, Friday. And as they go through the week, they're attempting to initiate conversation with him at my direction of, "Hey, you know, What's this for? Is everything okay? You know, is there a more secure way we could do whatever you need to do with this cash? You know, we can send a wire we can ACH this to somebody. You know, a cashier's check." Anything, but keep this, you know, 75-year-old man from walking out of our branch with a stack of hundreds in his pocket. Anytime he was in and was faced with questions on it, he would kind of become reticent, look at the ground and say it's for a family member in need. A normally very talkative friendly member is very reclusive about this situation, didn't want to answer any questions about it.

So, branch staff brings it to me. I start looking at it. And I see, you know, not cash-intensive and suddenly very cash-intensive. So, as I said, I'd only been at Elements about four months at that point. It hadn't really sunk in with me yet that I was no longer a detective. And you know, one of the things you do when your detective is sometimes you just go knock on somebody's door and say, "Hey, I'd like to talk to you about this."

So luckily for us, he lived, you know, in the Indianapolis area, so it wasn't too big of a jaunt for me to get up to his his retirement home. But I mean, I would have driven anywhere within reason to go find him. But it luckily wasn't too far away. So I check in at the front desk, and they tell him he's got a visitor and he comes down and lets me in and it was kind of a surreal experience. And he takes me up to his unit, and we sit down in his dining room table.

And, you know, to my dying day, I'll remember the words I said to him almost verbatim. And I said, "This is your money. You can do with it as you wish. You can pull it all out and throw it in a bonfire. I don't really want that to occur. But this is your money. You can ask me to leave at any time, and you have no obligation to share anything with me. But I believe you're being

defrauded. And I think you're the victim in a fraud scheme." And at this point, remember, I don't know what the scheme is. All I know is $2,000 cash has been coming out for a week straight. And so, I get into this very broad talk about how fraud schemes work, you know, the bad guy finds you. They convince you that there's something urgent. It could be a person you met online for companionship. It could be someone posing as a family member who's stranded. It could be a sweepstakes, or a lottery, all of the various the ways that we've seen this come about. And all the while I'm kind of staring him in the face, seeing if any of those up options kind of bring out a reaction in him. And he's pretty stone faced. He doesn't really give me much. But I could tell I was kind of over the target because he's kind of stewing on it a little bit. And as I as I go through how the mechanics of everything worked, you know, go figure, I actually stopped talking for once, and we sat there in silence.

And that's one of the oldest tricks from law enforcement is don't be afraid of the silence. And I could tell he was in a serious bind about what he should do. And I wanted him to deal with it at his own pace. And we sat there for probably 30 silent seconds that seemed like two hours. And he eventually said, "Well, I'm not supposed to tell you this, because I signed a confidentiality agreement, but I won a foreign lottery." At this point, yeah, at this point, I know, I know, we're over the target. I know we're on to something here. And it's up to me to try to pull them out of this.

And I know this from law enforcement and from my time at elements, getting someone to admit that they've been defrauded is one of the toughest psychological adventures you can ever go on, or psychological challenges. Because everybody says this will never happen to me. They see it on the news or they read stories about it and they say, "What a fool. Now how could they fall for that? That will never happen to me." Until it does.

So, he starts telling me the story. And again, another trick from law enforcement, you know, never pounce on the red flags until they've told you the entire story. So, he's telling me the story. Got the postcard sends it back in. He starts getting calls from 202 area code numbers that he equated with the federal government because that's D.C.'s area code. They claimed they were with the United States Department of Sweepstakes, you know, these kind of things that seemed legitimate to him, but were just bricks in the wall of trying to seem legitimate.

So, what he told me was he was guided by the bad guys that the first $2,000 withdrawal was for the taxes to Australia, so he had to take out money and then pay the taxes to all of the various countries that were participating in the international lottery scheme. You know, you play an international lottery and you win and international countries want their taxes. It kind of seems plausible when you're excited about the prospect of, you know, getting a half million dollar check. Day two is to the Maldives; day three is to Thailand; day four is to all these different places. And I told him and I'm showing him articles on my phone from Western Union, from the FBI from everybody that this is a standard common fraud scheme and that he is being defrauded. His money is gone. There's nothing Elements can do to help him with it because he took out cash and then sent it through Western Union.

And he said, “But I'm supposed to get my half million dollar check tomorrow.”

And it just breaks your heart. Because, you know, he's so conflicted at this point. He wants to believe the bad guys. I'm his dream-crusher coming in out of the blue. And I said, “You're not gonna get that check in. If you do, it's fraudulent. So don't bring it to Elements. We're going to put an enormous hold on it because it's not going to clear. But you're not going to get that check. And when you don't get that check tomorrow, I hope I gain a little bit of credibility in your eyes. You know, remember who has approached you about this entire situation. You've got the nameless, faceless, high-pressure people that you've never met, who all they want is, you know, $2,000 $2,000 $2,000, and it's never gonna stop. And you've got me on the other hand, who come to your apartment face to face. I asked for nothing from you. I've shown you my driver's license. I've shown you my business card from Elements. I'm a real person who is just trying to help you. And if my prediction that this check doesn't come, I hope I gain a little bit of credibility, and we can talk, talk more about this.”

I said, “Please don't send them any more money until you don't get this check tomorrow. And then let's talk again tomorrow.” So, he calls me up the next day and says, you know, “Check didn't come.” And, you know, I can't swear on this podcast. But I said, “No kidding.”

And, you know, we, we didn't laugh about it.

But I said, “Okay, are we ready to acknowledge that this is probably fraud?” and he wasn't quite ready yet. And I said, “Okay, well, put me in touch with these bad guys. Can we put me as your power of attorney or your personal representative or at least inject me into the mix that there's somebody looking over your shoulder to this?” So, he's like, “All right, I'll try.”

So, he said he, when he gets the next call from them, the next high-pressure call of the him owing money, he says, “Hey, Andy shank from Elements, my bank, says this is fraud. And he'd like to talk to you guys.” They come back and say, “Well, Andy Shank is a thief. He's trying to steal your money. We're the good guys. And now you breached your confidentiality agreement. And we're gonna report you to the FBI. Now you owe us $80,000 by the end of the month, or by the end of the week.”

So that was kind of the straw that broke the camel's back from him. He realized that it was fraud at that point. And he never sent them another dime, never answered their calls. And they kind of just faded away. But he was out about 13 grand at the end of the day, 13 grand that we were never able to get back and 13 grand that went to really bad guys. And the the part that really makes this story unique and memorable for me, because, you know, we dealt with multiple instances that are parallel this one in shape and form up to this point. But I got a call about four months later from law enforcement asking me about this. And the money that he was sending was going directly to an Al Qaeda sect in Thailand.

Lisa Hochgraf 55:51
Wow.

Andy Shank 55:52
So, yeah. So my entire law enforcement career, you know, I saw some crazy things, I got myself into some wild situations. But literally, the most jarring and frightening moment of my entire adult life was four months into my career at a credit union as a fraud victim is telling Al Qaeda, “Hey, Andy shank is stopping your money from getting to you.” So, I tell that story frequently because a) it's it's kind of sobering to think that, you know, these aren't just organized fraud rings who want to go buy a yacht and, you know, silly material possessions with this fraud money. These were terrorists. I mean, it was absolute terrorist group using his money to buy bombs and do terrorist activities. So that is why I take this stuff so seriously. That is why there is no incident that's too small to get a full investigation because I've seen where the money goes. And it's not just a kid buying a new Xbox in his mom's basement. It is really, really bad international terrorist organizations.

And I'm not saying every single fraud scheme routes back to terrorism. But I can say with firsthand assurance that it absolutely is possible and does frequently occur. So you know, my guidance for the credit unions out there would be take this seriously even if it's not going to hit your bottom line as as a credit union because even if if you are remiss in your monitoring and your approach to these kind of incidences, I will never go so far to say you're funding terrorism, but you have a duty to everybody to make sure that the bad guys have a very, very uphill battle to succeed.

And I offer this to everybody as well. You know, whether you're a Harland Clarke client or not: If you've got a situation that you would like to talk out with a fresh set of eyes of somebody who's been there, I am happy to help you guys, day in, day day or night, nights, weekends, whatever, because I I truly find my passion in life is stopping bad guys from getting money. And if if that takes me away from a normal work test to help a credit union or a bank somewhere keep a bad guy pockets empty, then everybody wins.

Lisa Hochgraf 57:45
And that member, that member. You helped that friendly man that was known to the tellers in the branch overcome being deceived. That was also a lovely part of your story.

Andy Shank 59:59
Yeah. And, you know, nobody ends up coming back and saying thank you because there's a certain level of shame that, you know, “Hey, I did get taken from it.” But you know, to me the the payback is just never seeing that activity on his account again. He gets back to being a frugal saver and spending his money at Walgreens and his church. You know, that was what was happening to me to see him getting back to normal. That's that's all the repayment I need.

Lisa Hochgraf 58:23
What an amazing story. Andy, thank you so much for telling it. And thank you so much for being on the show.

Andy Shank 58:29
Absolutely. Thank you for having me would love to come back again and get into more stories.

Lisa Hochgraf 59:33
I look forward to it.

Wow, I could really spend an entire afternoon hearing such great stories about fraud management. Thank you, Andy, for the terrific perspective on how to manage fraud, and for bringing it down to such a human level.

Thanks again to Harland Clarke for sponsoring this show. Harland Clarke is a CUES Supplier member based in San Antonio, Texas, and you can find them on the web at Harland clarke.com. That's h a r l a n d c l a r k e.com.

You might also be interested in learning more about CUES's upcoming online and in person learning programs. Find out more at cues.org/events.

If you're a CUES member, you have access to invaluable membership benefits to further enhance your development, many of which are available virtually. Visit cues.org slash membership to learn more. And of course, anyone listening can get more credit union specific content, but see you management com.

Thanks again for listening today.

CUES is an international credit union association. Our mission is to educate and develop credit union CEOs, executives, directors and future leaders. To learn how CUES can help you realize your potential, visit cues.org today.