Fraudcast: stories of tricks & treachery

Episode 6: Decrypting the truth

Jazz Clemente

Hello everyone and welcome to the KPMG Fraudcast, where we unravel fraud cases in the news to uncover what happened and explore lessons learned. My name is Jazz Clemente.

Frédéric LeBlond

And I'm Frédéric LeBlond.

Jazz Clemente

We are both Senior Consultants within the KPMG in Canada's Forensic practice.

Frédéric LeBlond

The stories we'll cover in this series are true events, but the names have been changed to aliases for the privacy of everyone involved. Although KPMG was not involved in these cases, we often work on cases similar to the ones of public knowledge we discuss. In this episode, we will be discussing stories of cryptocurrency fraud and how we can all protect ourselves from becoming victims.

The first story we'll discuss is about a Manitoba municipality and what ended up being a very bad holiday surprise. It illustrates the potential that cryptocurrencies have as an effective money laundering tool.

Jazz Clemente

Sounds like a true holiday story.

Frédéric LeBlond

It all started with a job advertisement targeting students and newcomers to Canada.

Jazz Clemente

Remember our first episode and our discussions about intimacy scams. Vulnerable people such as students and newcomers are easy targets for fraudsters.

Frédéric LeBlond

Absolutely, and although they're not the victim here, it's definitely no different. They're still being taken advantage of. This job posting was for a seemingly legitimate company with a professional website and a real address, claiming to be looking for cash processors one month contract, with work from home. This was shared on a number of major job websites where people typically look for postings. In total, 18 people were hired for this job. They were young and lived across Canada, but most were new Canadians. These employees were given an employment agreement that appeared very legitimate, including work conditions, job requirements, appropriate manager authorization and signatures, etc. Employees were told that they would receive payments on their credit cards, which they should then move to their own bank accounts. The payments should be withdrawn, converted to Bitcoin, and then sent to another account. In December 2019, the fraudsters sent a phishing email to several members of the municipality and at least one person clicked the link giving access to the municipality's computers and bank accounts.

Jazz Clemente

At that time, I'm sure nothing seemed suspicious yet.

Frédéric LeBlond

That's right, but never for long. Weeks went by, and nothing happened, so nothing was reported to the police. It was only later when the money started disappearing that they discovered the incidents were connected. On December 19, 2019, the fraudster logged into the bank account and changed the password and personal verification questions. They then added their 18 employees, as payees and began making systemic withdrawals, transferring money to the employee's credit cards for them to perform their quote unquote processing. 48 bank transfers were made to

unfamiliar accounts all under $10,000, totaling almost half a million dollars, a large portion of their $7 million annual budget.

Jazz Clemente

This is a classic case of structuring. Here, money launderers make multiple transactions just under the threshold being reviewed. In this case, that would be $10,000.

Frédéric LeBlond

And that's an important step in avoiding garnering unwanted attention from the banks. These transfers weren't discovered until January 6th when staff were back from holidays. The timing was surely no coincidence. The RCMP was informed, and the credit union was able to freeze and recover $50,000. The 18 workers were paid a commission on the cash conversion and sent out Bitcoin to what was identified as the private account of the scammers who were likely not in Canada. The municipalities sued their credit union and their insurance provider after the incident in an attempt to recoup their losses. And these lawsuits actually currently remain before the courts. The credit union's defense is that the municipality did not follow its request to have a forensic audit of their IT system and did not provide additional information when requested. While the insurance provider claims that there is no coverage for funds transfer fraud or computer fraud under their policy. Following this incident, the province also ordered an investigation by the Auditor General on the operations of various municipalities including this one.

The next story, a shorter one, is about YouTube ‘finfluencers’ and some of the risks of following the advice of these finance gurus.

Jazz Clemente

It's so easy to follow these bite-sized tips, especially since we are always on our phone scrolling. This would be a good reminder of why it is important not to trust these so-called online gurus immediately.

Frédéric LeBlond

Honestly, I'm always surprised by how much of this content I get myself.

Charles O'Connor was casually watching videos on YouTube, when he came across a video by someone who claimed his viewers could make a lot of money trading commodities, forex and cryptocurrencies. Intrigued he contacted the company responsible for the video, accessed their trading platform, and started off by investing a safe amount of $250. After seeing this amount grow, Charles felt confident investing an additional $2,500. He also made a thousand dollars withdrawal that went through just fine, and so he felt quite confident still. Over the next several months, Charles invested his life savings of $498,000. Little did he know the platform he was on was just a simulation. When it said his funds had grown to $1.3 million, he wanted to take some out, but then he was told he'd have to pay $150,000, quote unquote liquidation provision, realized he got conned. The victim had to sell his home and reorganize his whole life, having only about two to three months of usable cash left.

Jazz Clemente

Wow, this really shows that anything that seems too good to be true is probably too good to be true. This was definitely a lesson learned the hard way for him.

Frédéric LeBlond

Absolutely.

Frédéric LeBlond

The last story I'd like to discuss is that of the case against John Travis Jones and his failed crypto coin offering. This story illustrates some of the unique fraud risks to consider when investing in crypto. The Ontario Securities Commission, along with the SEC accused an Ontario man of a massive cryptocurrency fraud involving a crypto token offering where invested funds were misappropriated for personal use.

John Travis Jones and his companies promoted and sold a crypto asset named the Integrity Token for ING, which was previously known as Collabo Coin or CBC, two investors around the world raising $51 million US from investors.

Jazz Clemente

Crypto fraud is an emerging topic. I'm excited to hear how this story plays out.

Frédéric LeBlond

The premise of this story is that in 2017, Jones and his companies created a crypto security token named the Collabo coin, which was hosted on the Ethereum blockchain, which was issued on trading platforms, he had made arrangements with at the time. Promotional materials that were provided for this token by Jones' issuing companies made statements that investor funds would be used to

acquire crypto asset mining equipment, in order to generate proceeds that would then be used to buy gold bullion and additional mining equipment to create exponential growth in earnings and physical bullion holdings to back the CBC tokens. Each CBC token would be backed by a floor price of $1 US worth of gold, limiting risk and maximizing potential. The collabo coin was eventually renamed as the Integrity Token or ING. To break it down, there are two main features to this cryptocurrency that are worth noting. First off, investor funds were intended to be used to purchase gold bullion. This is important because gold bullion is a tangible commodity that is universally recognized as having sure and long-lasting value. Using such an asset to back a cryptocurrency provides security on an asset that is otherwise extremely volatile or of an unreliable value, if you will.

Jazz Clemente

Could you explain why having an asset backing is unique in this case?

Frédéric LeBlond

Absolutely. So crypto tokens like Bitcoin aren't directly backed by a physical asset like in this case, and so their value is much more speculative, which means it is essentially whatever people as a group decide that it's worth, effectively. But since this token is backed by gold and in this case at least a dollar's worth of gold per token, investors consider the inherent value of that gold, along with the token making things less speculative and thus less volatile. This is attractive to investors. Second, investor funds were also intended to be reinvested into cryptocurrency mining equipment. Cryptocurrency mining is a process by which crypto tokens enter into circulation. Simply put, it involves using computers to solve complex computational problems that upkeep the crypto systems maintenance and development and rewards those who solve them with lucrative crypto coins. The computing power required to do this is quite high, and so a lot of expensive computing equipment and energy is required to do so. So basically, they would use investor funds to buy computer equipment, hopefully successfully mine some coins, sell them and then buy more gold bullion to further secure the token and more equipment to mine exponentially more coins.

Jazz Clemente

This is very interesting, Fred. There's definitely a lot of information here. Perhaps you could give a quick summary to our listeners?

Frédéric LeBlond

I totally get it. Let me break it down simply. So, say you were selling this coin and my nine friends, and I bought this coin from you for a hundred dollars each. The $1,000 we gave you for this coin, you take it, and you use 500 bucks to buy gold. Then you say, okay, each of you are basically holding a cut of this gold as part of your investment and that makes us happy because gold is stable. Now you're left with $500. So, you take that money and buy crypto mining equipment. That equipment will let you earn crypto for your effort and give you more money with which you will keep buying more gold and buying mining equipment to earn even more money. And this cycle continues and me as an investor, I'm hoping the work you're putting in will make my investment worth more over time.

Now onto the problems. One of Jones's companies said they had agreed to purchase $10 million US of gold from a company called Sonar Bullion FZW based in the United Arab Emirates, but the agreement was missing several key details including the purchase price, and the company never actually owned the Gold Bullion it had apparently pledged. Despite the millions of dollars invested, none of Jones's companies ever purchased gold from Sonar or otherwise owned any gold at all. The gold bullion promise ended up being one of several false or misleading statements found in the promotional materials. On top of that, ING and CBC were primarily purchased with Bitcoin, which was exchanged to USD by one of Jones' accomplices and distributed to various parties including Jones, who received millions of dollars directly and indirectly. Some of the funds were indeed used for mining equipment, but a significant amount was depleted for unrelated purposes. These include acquiring and improving real estate in Ontario, purchasing luxury motorboats, making payments to bank accounts controlled by Jones or to parties for the benefit of Jones, buying a property in Bermuda and paying monthly fees for the so-called gold pledging agreement with sonar. In addition, the OSC also alleges that they never filed a prospectus regarding the distribution of the integrity token and did not properly register with them to engage in trading. Had they registered properly, the scheme would've likely been found out.

Enforcement staff at the OSC are asking commissioners to order Jones to pay an administrative penalty, no more than

$1 million for each failure to comply with Ontario Securities law with similar penalties envisioned by the SEC and the US.

Frédéric LeBlond

Today I'm very excited to introduce our guests for this episode, Amrit Dev and James Emerson. Amrit has recently rejoined the team after spending time in the enforcement division at the Ontario Securities Commission, where she got experience investigating various rug pull and investment scams, hacks, unregistered activity, and market manipulation as it relates to crypto assets and DeFi. James is a manager in KPMG Canada's crypto assets and blockchain COE. He has been actively involved in the digital asset space for more than four years and has designed, developed and operated several digital assets mining nodes, including Ethereum nodes. James has over six years of experience in delivering engagements for large publicly traded digital asset funds, private financial institutions, and crypto native companies.

So as an emerging technology crypto is both incredibly interesting and intimidating at the same time. What do you guys think should investors be careful of when investing in cryptocurrencies?

James Emerson

Thanks, Fred. That's a great question and maybe I'll take the first stab at it. There are currently more than 8,000 different crypto assets that are available for purchase at this time. While many of these projects are attending to provide value and innovate, others are simply just a way for project creators to make quick money from unsuspecting investors or outright scams. Investors should do appropriate due diligence just like they would for any traditional financial investment. Due diligence is about gathering as much information as possible to make an informed decision, and it's the foundation of smart investing in the crypto space. If you've identified a potential crypto asset investment, one of the first steps you should take is to research the business model. You want to look at the project's white paper and see if it holds up under scrutiny. The white paper should also clearly identify what the objective of the project is, the team, the timelines, the value that is being added, whether the project has obtained the appropriate licenses to operate in the specific jurisdiction, registered with the relevant regulators and find how relevant risks will be mitigated.

Other things you should also consider include whether the timeline for development launch and expansion are reasonable, are there any glaring holes or issues with the developer's plans? You also want to consider whether the token, can be purchased in your specific jurisdiction. Sometimes projects only offer the ability for investors in certain allowed jurisdictions to make investment.

Another key area of focus should be on the development team itself. It's very important to do research on who the key team members are, what their experience is, and whether they have a good track record in the space. A strong transparent team is a good sign. Also, you want to assess the community and the ecosystem around the crypto asset. A vibrant, active online community can be a positive indicator and also keep an eye out on whether there are any VCs or private equity funds that have made investments in the project in its initial phases. By doing this research, you can get a better idea if professional investors in the space are also back in the project.

I'll pass it off to Amrit now to share her thoughts as well.

Amrit Dev

Thanks, James. I think the point around doing your due diligence is super critical and I want to highlight two reasons why doing your own due diligence is important. First, what we're seeing is that a first-time victim to a fraudulent crypto asset investment scheme is likely to fall prey to yet another one by the same scammers who try to either relaunch a 2.0 version of the same investment schemes or rebrand themselves as a scam recovery service. Something else you want to be careful about is the irreversible nature of blockchain transactions. Once you make a payment to a wrong address or a scammer even through an exchange, once that payment is processed, it cannot be reversed. You don't have the same protections you may with a bank, in the case of crypto assets. If you're looking to invest or trade crypto assets, look for exchanges that have been registered by CSA or are currently seeking registration.

CSA is Canadian Securities Administrators and a list of these compliant exchanges or exchanges seeking administration can be found on CSA's website. These exchanges are required by provincial securities regulators to abide by certain conditions to help protect investors. There are various protections that are available, but just to highlight some of them, these would include things like implementing custody controls to help protect crypto assets for customers. This may include limiting the types of crypto assets that are being traded on these exchanges so that high risk tokens

and assets are not eligible for trading on these platforms, and also, they're required to meet obligation to clients, including obligation to deliver crypto assets upon client's request. These are some of the exchanges that you can look to trade or invest on, by looking at the CSAs website.

Frédéric LeBlond

Thanks to you both, that was very interesting, and I think it truly highlights the point that, you know, we should really only invest in things that we truly understand and sometimes that takes time and research and due diligence like you both said. Could you guys tell me a little bit more about what role does KPMG play in this industry?

Amrit Dev

Yeah, for sure. Thanks, Fred. Our forensic team offers a multitude of services. There are anti-money laundering compliance services that we provide to customers. We also provide asset tracing investigation and dispute advisory services in this space. We do this by bringing a multidisciplinary team to the client, as we have forensic and financial crime professionals, who bring the regulatory compliance, forensic accounting and dispute advisory lens to an investigation. And we often work with professionals from our crypto asset COE team, which is James' team, who provide the technical crypto knowledge. And I'll pass it off to James to speak a little bit more about his team.

James Emerson

Thanks Amrit. The most common way people find themselves becoming victim to crypto scams are either by transferring dollars from their bank accounts into fraudulent or unlicensed crypto exchanges, what we often call high risk venues or by sending their crypto holdings from their account on a crypto exchange, to a fraudster's wallet unwittingly or unknowingly. Misappropriated Crypto assets typically get laundered through chain hopping mixers, peer-to-peer platforms and noncompliant exchanges. What fraudsters often do is mix the stolen assets with other users to make detection more difficult. These illicit actors then look for ways to off ramp the laundered crypto asset, and often they do this by converting the laundered proceeds into fiat currency through centralized exchanges. Both of the crypto scam techniques that I just mentioned can be avoided, if banks and crypto trading platforms have adequate compliance programs and crypto intelligence tools respectively, to identify, flag and block these transactions, on behalf of their customers and inform customers in a timely manner. KPMG in Canada's crypto and blockchain Center of Excellence has a dedicated team of crypto subject matter experts, and we work closely with Amrit's team. We specialize in helping banks in crypto trading platforms with enabling and updating their compliance programs and implementing and configuration of crypto intelligence tools or prevention before an incident occurs and investigation post detection of these kind of incidents. We also have a wide range of service offerings from educational models, assisting with licensing and regulatory compliance, development of risk frameworks and policies and exchange in custody integration.

Frédéric LeBlond

Wow, that was some excellent information. Thanks so much for joining us today, James and Amrit.

Jazz Clemente

Each episode, we'd like to leave you with a little something to help increase fraud awareness. Here is Fred with our fraud scheme of the week, the infamous pump and dump, also known as a rug pull scheme.

Frédéric LeBlond

Pump and dumps are not new. They've existed for a long time and can also be performed on the stock market. A famous example of this would be the Wolf of Wall Street who would inflate stock prices of unregulated penny stocks, which he secretly owned. He would then sell them before anyone else would, leaving investors with near worthless shares.

Crypto has brought forth an unfortunate revival of the scheme, but to proportions never seen before. Crypto coins are created left and right. They're sponsored by celebrities and other public figures on social media and have values that are often purely speculative, the perfect recipe for pump and dump smash success.

Jazz Clemente

So how do you manage this?

Frédéric LeBlond

To manage these properly, you need to learn these warning signs to spot crypto scams before you become a victim yourself. First off, guaranteed returns. No one can predict the future, and thus no one can guarantee returns on an investment. If a guaranteed return is promised, tread carefully. Then, excessive marketing. Heavy marketing

featuring high levels of pressure is one of, if not the clearest sign of a pump and dump. Next, unnamed team members. You should be able to learn about the key people behind the cryptocurrency. And last but not least, free money. If you are offered free money, it's very likely to be fake. If it's too good to be true, it probably is. And as with most investments, you should do your research, only invest in things you understand and take your time in doing so.

KPMG Forensic professionals transform how clients identify, mitigate, and respond to risk, saving time and money. We help individuals and organizations stay on top of fraud, and we would love to help you too. On behalf of the whole KPMG Regions East forensic team, thank you very much for tuning into this episode of the KPMG Fraudcast.

Jazz Clemente

And we hope you join us again next time.