aunalytics

The Visible and Invisible Risks of Cryptocurrency for Banks and Credit Unions

By: Katie Horvath, CMO Aunalytics

As cryptocurrency ads dominated the Super Bowl, resulting in a reported 247% increase in new users signing up on cryptocurrency exchange apps, financial institutions should be on high alert for the alarming increase in both visible and hidden risks to their institutions.

The allure of investing early in the "next big thing" has led to increased interest in crypto investment. As a new industry, it is highly unregulated compared to other types of investments and banking. While there is potential for a big win, there is strong potential for a big lose.

As a bank or credit union, here's what you need to know to protect your institution.

Visible Risk: Which of Your Customers are Drawn to Crypto?

Which of your customers is at risk for moving investment dollars away from your institution to crypto? Which of your customers have investments with crypto firms?

If you do not know the answer to these questions, you need a data analytics solution that mines your transactional banking data to tell you which of your customers are pulling dollars from your bank and putting them into crypto exchanges and investments. While this level of technology is known in big banking, there now are data analytics products built specifically for mid-market financial institutions to give you this level of insight into your customers or members.

One group to keep an eye on includes younger adults, years away from retirement. They decide to put money into a cryptocurrency investment with the idea that the currency will gain value over time. When compared to current low and no interest checking and savings account rates, where money will not grow in a conventional banking account, crypto provides the promise of exponential growth. These customers are not worried about stability in retirement because to them, retirement is still years away.

Factors such as risk toleration and more can be used in predictive analytics to see which of your members are more likely to make crypto investments. This type of investment attracts adrenaline junkies, risk takers, gamblers, those looking for big pay offs, and typically not the profile used for likely bond investors.

Customer behaviors can be mined to determine who is involved in crypto. Data analytics solutions built for mid-market bankers (not just available to banking giants) provide on-demand customer intelligence. For example, you can use natural language to ask data analytics, "which of my customers have crypto investments" or "which of my members are most likely to purchase crypto" and receive an answer in minutes for you to act upon. Analytics products built for credit unions and mid-market banks offer this granular level of insights as a service to inform banking strategies.

Visible Crypto Risk: Losing Investment Dollars

Financial institutions are concerned with how to compete against crypto for investment dollars. For example, how do you introduce an attractive investment offer to compete with crypto options and keep your customers' dollars in your bank? Perhaps your institution has a product that would be attractive to a crypto buyer. If so, having visibility into which customers to target and win over those investment dollars is very valuable.

Visible Crypto Risk: Fraud

When we think about crypto investments, we typically worry about fraud.

Online con artists create attractive offers aimed at millennials and Gen Z'ers, who perceive this type of investment as hip, cool, and brag-worthy, with a potentially huge upside if the crypto lottery lands them a unicorn. We often hear about fraud where unscrupulous bad actors steal customer money in a scheme surrounding a fake currency that does not really exist. This type of classic fraud is based upon the concept of buying a product online that does not exist—and you've lost your money. As with most industries having a private sector, there are good actors and bad actors alike. This type of fraud is a risk anywhere. However, cryptocurrency is particularly a risk because:

The crime has a valuable reward:

- This is a financial transaction where cybercriminals can quickly get money as a reward for the crime.
- Criminals also receive valuable bank accounts and other personal information as a reward for the crime, which can be further exploited for added profit.

No barriers are standing in the way:

- Easy entry into the industry enables bad actors to get in front of consumers due to lack of government regulation.
- There is little recourse for consumers due to lack of fraud protection backing crypto purchases.
- As an emerging industry, new names are often popping up that are not automatically flagging potential fraud.

Exchange sites aim to minimize consumer risks, but crypto is still in the wild, wild west stage. While some crypto investment opportunities may be speculative long-term plays, unfortunately, unscrupulous scammers have been attracted to this emerging industry. Investors may find their investment to be worth nothing when the value is stolen by a scammer. New cryptocurrency brands emerge often and many consumers have no idea which are legitimate.

> Because cryptocurrency is stored in a digital wallet, it is vulnerable to theft. There is no banking intermediary or anyone else to turn to in the event of fraud.

Because cryptocurrency is stored in a digital wallet, it is vulnerable to theft. There is no banking intermediary or anyone else to turn to in the event of fraud. Cryptocurrency is not backed by the government and unlike credit card purchases, returns and refunds are often not possible because the unregulated industry does not offer these protections as standard. People use cryptocurrency for quick payments, to avoid transaction fees that regular banks charge, or because it offers some anonymity. It is typically exchanged person to person online (such as over a phone or computer) without an intermediary like a bank. This means that there is often no one to turn to if there is a problem with the exchange. So, if your customer stores crypto with a third-party company that disappears or is hacked and the customer's money is stolen, there is little to no recourse and the government has no obligation to help get the money back.

Even with legitimate crypto investments, currency values change rapidly and constantly. Value is based upon supply and demand. Unlike many investments that may fall in value but typically regain value over time, crypto is less stable. A purchase of $1,000 could fall to a value of $100 in minutes. Conversely, it could rise to a value of $10,000 in minutes. But then it could change again—even while your customer is trying to cash out on a gain while up, it could result in a loss due to the value changing again before the transaction is complete.

So, who does your customer turn to with complaints if his crypto investment turns out to be fraud and his bank account gets cleaned out, or her money is lost due to the time it takes for a transaction to complete? With lack of regulation, there is no one for your customer to turn to but you. Crypto fraud becomes your operational cost. Crypto fraud lowers your customer satisfaction scores. As the only man standing, your bank unfairly becomes the target of your customer's anger, embarrassment, and bad gamble.

How Can You Protect Your Customers from Crypto Fraud?

As a financial institution, knowing which customers are at risk for fraud presents an actionable insight that allows you to take proactive steps. You can educate those customers and make them more aware of crypto risk, how to stop fraud, and hopefully prevent them from falling victim to these scams. Furthermore, taking proactive measures based on data analytics intelligence helps prevent the operational cost to your bank or credit union by having to deal with crypto fraud incidences.

Rather than training employees with scripts for merely empathizing with customers while deflecting responsibility when crypto fraud occurs, educate customers away from risk and fraud by explaining that no regulation means no one has their back. In this manner you can mitigate customer complaints (after all, you tried to warn them), and hopefully reduce operational costs in dealing with crypto fraud fall-out.

Data analytics can mine your transactional data to determine which of your customers has money leaving or entering your bank from a cryptocurrency company. This will give you an actionable list of customers for outreach and education on risks. If enriched with a listing of crypto companies known to be fraudulent, conduct targeted outreach to save your customers from fraud. Further, after explaining the risks of crypto and educating your customers, you may be able to offer an alternative investment opportunity to keep them safe and their dollars in your bank.

Hidden Crypto Risk: Cyber Security

The biggest risk created by crypto for your institution is cybersecurity.

Since crypto is an emerging industry, new company names frequently appear to introduce new service offerings, creating the expectation that just because a company name is unfamiliar, doesn't mean it is automatically suspicious. Consumers are less wary of email soliciting their investment in crypto, even though it may be from an unknown company. Clicking on the wrong link or opening the wrong attachment can compromise the security of devices, networks, servers, and most importantly, data. Consumers are more likely to click on a link from an unknown person or company when it has to do with an emerging industry where new and unknown names are common. Cybercriminals, in fact, seek out this area of vulnerability when devising campaigns.

Customers involved with crypto are more vulnerable to having their credentials stolen to gain access to bank accounts, and are more likely to be impersonated by bad actors. Well-intentioned customer service actions by your employees to help these "customers" leads to cyber criminals penetrating your bank's systems and security.

> In 2020, attacks against banks and other financial institutions climbed an incredible 238% followed by a 118% increase in 2021.

For the past six years, the finance sector has been ranked #1 as the most cyberattacked industry. Even so, in 2020, attacks against banks and other financial institutions climbed an incredible 238% followed by a further impressive 118% increase in 2021. Cyber criminals continue to double down efforts to breach financial data, compromise accounts, and profit from this industry with increasingly sophisticated attacks and campaigns. It is no surprise, given that banking enterprises hold a lot of sensitive data about people, companies and governments, and their transactional business revolves around massive volumes of money transfer.

All of this presents a huge opportunity for hackers to hide from detection until funds and valuable data are stolen. Hackers will continue to strike with increasing sophistication since the data held by financial institutions is high value with the potential for extremely lucrative financial gains if stolen.

According to the 2021 Modern Bank Heists 4.0 survey, the most common types of attacks hitting the financial services sector in 2020 and 2021 included server attacks, data theft, and ransomware cases. It was also found that 57% of surveyed financial institutions revealed an increase in wire transfer fraud, 54% had experienced destructive attacks, 41% had suffered brokerage account take-overs, 51% experienced attacks on target market strategy data, 38% suffered attacks originating from hackers accessing trusted supply chain partners to gain entry into the bank, and 41% had become victim to manipulated timestamps resulting in fund theft.

> 57% of surveyed financial institutions revealed an increase in wire transfer fraud
>
> *- 2021 Modern Bank Heists 4.0*

In many new highly sophisticated attacks, cybercriminals get into systems by impersonating a vendor or customer that regularly does business with your financial institution. Individuals let their guard down when they see a familiar, credible entity associated with email or other types of outreach. Your banking customer could really be a crypto scammer impersonating your customer. Since the crypto industry is both emerging and unregulated, it poses a double threat, driving up the risk of impersonation and fraud. You need to know which customers are attracted to crypto so you can better defend your institution.

Next, many new sophisticated cyberattacks include penetrating security, followed by sitting, listening, learning, and looking for where the most valuable data is stored before attacking. You may have cyber criminals accessing your internal banking systems today, lying in wait and planning an attack from the inside. Heightened account monitoring of members or customers who are into crypto is advisable.

Most financial institution IT teams are chronically understaffed and under pressure to introduce new technologies with compressed deadlines. Using data analytics for increased intelligence is key to identifying which customers and accounts are at risk and require careful surveillance for cyberattacks. A crypto fraudster impersonating a member might send an email to one of your unsuspecting credit union employees containing a link, an attachment or the like. Your employee, particularly in community banking where members are accustomed to white glove service, is more likely to respond to the email or trust the attachment. Then the silent hidden countdown starts, until the bomb explodes.

Ask yourself—does your institution have the time and resources to keep pace with ever-shifting cybersecurity threats and trends? Are you better able to identify and protect against known vulnerabilities or hidden vulnerabilities? According to Tom Scholtz, Distinguished VP Analyst at Gartner, "Organizations are struggling to keep up with the current threat landscape. Too many manual processes are in place, and security and risk managers must wrestle with a lack of resources, skills and budgets."

We saw cyberattacks growing in volume exponentially in 2021. Cyber criminals tried to take advantage of a newly distributed remote workforce to steal sensitive data. The focus shifted overnight from perimeters to device and user-based authentication, dual factor authentication became standard, and zero trust strategies were prioritized. Heading into 2022, many banks have quick IT fixes made during 2021 in need of fortification. Many have not kept current with patches for vulnerabilities.

Do you know what cyber threats are likely attacking your business this week? Has your IT department had time to train your entire company to be on alert for the latest phishing, smishing and vishing criminal campaigns for Q2 2022? Are you ready for the next attack?

> CISOs are expected to selectively add more than 30 capabilities to their function over the next 24 months
>
> *- Gartner*

Have you updated your detection and prevention plan, response strategy and remediation plan for 2022 threats? Is your identity verification dynamic? Are you using anti-phishing behavior management? Email gateway protection?

The unemployment rate for IT security professionals is approximately zero. According to Gartner, while the demand for security professionals continues to grow, the number of people with the skills and experience required to fill these positions is not keeping pace. It's difficult to hire new security talent. It takes an average of 130 days to fill open IT security positions; openings go unfilled and teams remain understaffed for many months.

Yet for 2022, new security capabilities and roles are required. Digitalization in banking is driving the need for new skills and knowledge of IT security, and the scarcity of skills is compounded by the volume of emerging threats. At the same time, IT security teams are expected to play a larger strategic role, balancing risk with growth using new technologies, while meeting the growing demand for information security support. Gartner reports that CISOs are expected to selectively add more than 30 capabilities to their function over the next 24 months, becoming increasingly responsible for setting security strategy and informing enterprise-wide strategy.

Security must now be embedded in all IT services. Can you meet your institution's needs and establish solid detection, response, and remediation strategies with continuous education, evolving safeguards, and moving (removing?) target threats? Are banking cybersecurity issues serious enough to become your main business focus instead of banking?

Given the economy, jobs report, scarcity of highly skilled security experts, Talent War of 2022, increasing threat and attack landscape and ever-changing strategies, skills and knowledge needed to keep current in mitigating against cyberattacks, 2022 points to more companies adopting managed security services to enhance their IT teams. Managed security services provide security experts that your in-house IT and security teams can leverage. Security experts bring advanced monitoring, detection and response technologies and it is their job to keep up with the latest trends and threats.

Most banking IT and security departments cannot respond to attacks to bring services back on-line as fast as managed services security experts do, and they struggle to stay current due to lack of time or people, given the exploding threat landscape. Data analytics enables you to pinpoint areas of high risk, such as customers who are, or who are likely to get involved with crypto, so you can better protect your institution with limited security resources.

Crypto puts banking institutions at greater risk than ever before at a time when cyberattacks are reaching new levels of sophistication, and monitoring and remediation resources are scarce. Cybersecurity is a hidden risk that comes with crypto, and data analytics, coupled with managed services and security experts, can help mitigate. Providing overworked IT and security teams the ability to identify customers who are inadvertently creating cyber risk will help them better target their efforts and protect your financial institution.

About Aunalytics

Aunalytics is the data platform company delivering answers for your business. Aunalytics provides Insights-as-a-Service to answer enterprise and midsized companies' most important IT and business questions. The Aunalytics® cloud-native data platform is built for universal data access, advanced analytics and AI while unifying disparate data silos into a single golden record of accurate, actionable business information. Its Daybreak™ industry intelligent data mart combined with the power of the Aunalytics data platform provides industry-specific data models with built-in queries and AI to ensure access to timely, accurate data and answers to critical business and IT questions. Through its side-by-side digital transformation model, Aunalytics provides on-demand scalable access to technology, data science, and AI experts to seamlessly transform customers businesses. To learn more contact us at +1 855-799-DATA or visit Aunalytics at https://www.aunalytics.com or on Twitter and LinkedIn.