UBB First for Your Success™

News, Analysis and Perspective for Community Banks by the Nation's **First** Bankers' Bank

Independent

Fall 2022

A Quarterly Publication of United Bankers' Bank

Member FDIC

This Issue:

Cybersecurity in the Banking Industry

By BlueTeam Alpha

In the last 10 to 15 years, the importance of cybersecurity has increased dramatically within the banking industry. Security will continue to play a more significant role in banking, especially with the continued digitization of the industry. The financial industry is one of the most vulnerable sectors to cyberattacks, but putting preventative measures in place can make a huge difference in the likelihood of an attack occurring and the amount of damage caused to the business.

Why Financial Institutions are Targets of Cyberattacks

The average cost of a data breach in the finance industry in 2022 is $5.97 million. This is the second highest average data breach cost across all sectors, making the financial industry a profitable target for cybercriminals. Its data is precious. Banks, investment firms, and credit card companies collect customer and client personally identifiable information (PII) with the understanding that these institutions will keep their data safe. But for cybercriminals, an attack on a business in this industry can have a considerable and widespread impact making the reward worth the risk.

Another reason the finance industry is often a target is the availability and ease of access to business platforms used by financial institutions. One significant benefit of technology is reaching more people and working with more customers. However, this widespread access also makes users more vulnerable. In addition, introducing new financial technologies increases the risk of hackers using this new technology to take control of legacy systems.

Cybersecurity continued pg 2

Dwight Larsen A note from the President

The old adage that "time flies" has proven to be true. It seems like it was just yesterday when we were welcoming in the start of summer and anticipating the fun networking opportunities of the packed event season to come. Now as I look out my office window and see leaves changing colors, I think back on all of the memories and connections made over the course of the summer and early fall at the events we had the privilege of hosting and attending.

Computers and the internet have revolutionized many facets of our lives, from how we communicate, watch television and listen to music, to how we purchase goods and services and conduct our banking. While the internet offers considerable time-saving benefits, it also offers cyber criminals opportunities to steal personal information and data while disrupting important computer systems. In this issue's cover story, UBB's Cybersecurity partner, BlueTeam Alpha, discusses the importance of strong training and awareness of cybersecurity threats in the banking industry.

Fraudsters have shown the ability to keep up with the fast-paced growth of technology and are regularly developing new tools and methods to steal sensitive data. This ongoing threat may make the questions and tactics you use to verify a customer's identity less effective and they may not work as well today as they did 10, 5, or even 1 year ago. UBB's Operations Team wants to help you strengthen your defenses by providing you with some suggestions for other qualifying questions to ask your customers and reminding you of the red flags of wire fraud to watch out for. This helpful article can be found on page 7.

Our Instant Payments Q&A provides information to help you determine the best instant payment provider for your bank and customers.

Vice President and Senior Compliance Consultant, Katie Ferrell, lays out the history and importance of Unfair, Deceptive, or Abusive Acts and Practices (UDAAP) as well as how to clear out the haze to understand a UDAAP risk assessment.

This past May, UBB welcomed Michael Hahn as Vice President, Correspondent Banking Officer serving the states of Montana, Nebraska, South Dakota, and Wyoming. Learn more about Michael on page 4 in the Employee Spotlight, then flip over to page 6 to learn how The National Bank of Germantown is *Keeping the Community in Community Banking*.

A wise person once said, "Autumn reminds us to see the beauty in change." However, one thing that will never change is that UBB will always be *First for Your Success*.

Cybersecurity trends and predictions

Upper management is playing a more significant role in cybersecurity.

Historically, decisions regarding cybersecurity in the banking industry have been driven by a company's IT department. That mindset is shifting today. Upper management plays a more significant role in cybersecurity in the industry than ever before. All relevant stakeholders need to come together to understand cybersecurity and make informed decisions around the subject. This is the best way to protect the data and assets of a company and make sure all systems are up and running.

Understanding how cyber insurance fits into your incident response plan

Having cyber insurance is an important step for businesses. It is important to understand what exactly your cyber insurance policy does and does not cover, so you can best protect your data accordingly. What is more important is understanding what to do when under attack. What is the first call to make in the event of a cyber incident? Do you have an internal team dedicated to help in the event of a cyberattack and are roles clearly defined? Having an incident response plan will enable you to respond faster to the threat and limit the amount of damage an attack can cause.

Outsourcing

In years past, banks handled more work in-house. Now, it's more common to outsource. This trend makes third-party vendor due diligence more crucial than ever. Banks must monitor their vendors carefully to ensure they comply with security policies and standards. Vendors can pose a significant risk if they have weaker security protocols. Banks should ask vendors for a SOC 2 – Type 2 report to verify their security.

While a bank might have excellent security, a partner with weaker security standards increases the likelihood of an attack. The lower standards affect the partner and the bank, so it's in the bank's best interest to ensure compliance.

Increased awareness and training

Banks need to implement more awareness and training. We also want to stress that these are separate critical defense mechanisms. Security awareness teaches employees what to look for and to identify red flags. Security training focuses on action and teaches employees what to do after discovering a red flag.

Separating IT and security

Big banks are beginning to hire designated cybersecurity teams, and this trend will become a best practice for the industry. IT professionals are skilled at many things, but security is a specialty subject best handled by a professional with experience and security certifications.

Small to mid-sized banks can partner with third-party security teams that integrate and work with existing IT systems and staff, which is more effective and affordable.

More penetration testing

As banks and their security programs mature, they will begin to see the value of frequent pen tests, both virtual and physical. Rotating pen testers every few years is also essential since each company has different pen testing methods. Banks should look for companies that provide thorough reports with actionable items.

In conclusion, with the cybersecurity landscape changing across the industry, threat actors are becoming more innovative, and security teams must keep this in mind. Banks must devote more time and resources to employee security training and awareness programs and put more proactive measures in place to limit their exposure to cyberattacks.

Restoring the Shine to Your UDAAP Lens

By Kathryn "Katie" Ferrell, CRCM, CAMS

Imagine walking into the sweltering heat after being in an air conditioned room, and your eyewear becomes incredibly foggy with condensation. Using the tail of your shirt, glasses are cleaned and repositioned on the eyes. Voila! Operations resume. Since the Consumer Federal Protection Bureau's (CFPB) formation, the Unfair, Deceptive, or Abusive Acts and Practices (UDAAP) journey reminds me of walking out of the air conditioning and into the heat over and over due to vague guidance and mixed signals from the agency that are followed by moments of clarity.

Understanding the UDAAP Evolution

Let's travel down memory lane. In 1938, Section 5 of the Federal Trade Commission (FTC) Act made it official that consumers deserve the right to be treated fairly when engaging in commerce across all industries. Sixty-six years later, the acronym "UDAP" was born, and the FTC used its authority to act on companies that treated consumers unfairly or deceptively.

When Congress passed the Dodd Frank Act and the CFPB was formed in 2010, the banking industry became more up close and personal with UDAP when enforcement of its violations and rulemaking transitioned from the FTC to the CFPB. The agency's first line of business was the introduction of the "abusive" prong, which expanded the acronym to UDAAP. For those of us serving in the industry in 2011, UDAAP was the buzzword, and banks braced for impact in response to what was and is still described as a very vague regulation. Training, policies, and risk assessments were implemented, and some banks named a "UDAAP Officer." Enforcement actions were taken under the director of the CFPB from 2012-2017 when authority was used to act on conduct that, until that time, no one knew was illegal, hence the popular "We know UDAAP when we see it" phrase. When a new administration took office in Washington in 2017, the CFPB loosened its reigns, and UDAAP enforcement declined under new directors and orders from the White House. In 2020, the acting director defined abusive in a Policy Statement which relieved institutions from civil penalties if good faith efforts to comply with the law were demonstrated. That Policy Statement was quickly rescinded when a new administration took office in 2021. UDAAP conversations regained momentum in public speeches, and the President signed an Executive Order (EO) encouraging the CFPB to revive enforcement of the law.

UDAAP Today

Since the EO and the permanent appointment of a new director, the CFPB's UDAAP Examination Procedures manual was updated to reflect a commitment to enforcement upon industry players accused of being unfair, deceptive, or abusive to consumers. A UDAAP violation is independent of other regulatory violations, and the CFPB has made it very clear that discrimination associated with any financial product, not just credit, is illegal. This includes deposit accounts, payments, and debt collections expanding further to include marketing, incentive programs, and any area of operations. The CFPB has publicly stated it will crack down on violations in home loans and small business loans. Even lending decisions using artificial intelligence and machine learning will be evaluated for UDAAP violations.

Managing UDAAP Risk During Times of Uncertainty

Although the UDAAP journey has provided both haze and clarity, success is achieved by continually wearing the UDAAP lens. Considering UDAAP at all stages of product evolution and throughout a consumer's entire banking journey with your institution is key. From the first introduction of your brand and offerings through marketing and advertising to the loan collections process and beyond, understand each area's susceptibility to UDAAP risk.

UDAAP continued pg 5

United Bankers' Bank
Call Report (unaudited)
6/30/2022

Balance Sheet (000's)	
Assets:	
Cash and Due from Banks	$ 261,944
Investments	$ 233,870
Fed Funds Sold & Securities Purchased Under Agreement to Resell	$ 68,617
Loans	
Outstanding	$ 697,739
Loss Reserve	$ (11,660)
Other Assets	$ 43,452
TOTAL ASSETS	$1,293,962
Liabilities and Capital:	
Deposits	$ 653,103
Fed Funds Purchased	$ 515,002
Other Liabilities	$ 9,074
Equity Capital	$ 116,783
TOTAL LIABILITIES & CAPITAL	$1,293,962

INCOME STATEMENT (YTD)	
Interest Income	$ 14,781
Interest Expense	$ 849
Net Interest Income	$ 13,932
Loss Provision	$ –
Net Interest Income (After Provision)	$ 13,932
Other Income	$ 10,437
Total Income	$ 24,369
Operating Expenses	$ 16,703
Securities Gains (Losses)	$ –
Net Income Before Taxes	$ 7,666
Tax	$ 2,008
NET INCOME	$ 5,658

Employee Spotlight

Michael Hahn

Vice President, Correspondent Banking Officer
605-291-2560 • michael.hahn@ubb.com

Family Members: Son, Will (8), and daughter, Claire (4).

Pets: None.

What do you listen to on your drive to work: Mostly podcasts with content centered around Gopher sports, college football, or true crime.

Interests: Golf, University of Minnesota Sports, college football and basketball, March Madness, candy, Tito's vodka.

If I could live anywhere in the world, I would live in: Assuming money isn't an issue, I would live in Hawaii near a golf course.

If I could have one super power (besides flying), it would be: Teleportation - it would make my job a lot easier.

Many people don't know that: I am from a very small family. I only have 1 first cousin on my mom's side. My dad is an only child.

If I was not working in banking, I would: Be working in a college athletic department.

I started working at UBB in: April 2022.

My favorite part of working for UBB: The people. Everyone is very helpful and easy to work with. Also, UBB's reputation in the industry and the banks in the states I call on.

The best advice I ever got was: Things turn out best for the people who make the best of the way things turn out.

First For Your Success means: All boats rise with the tide. A collaborative, relationship based approach to business helps everyone succeed.

Michael with Will and Claire at Storybook Island in Rapid City, SD.

Michael with his family at Disney World.

UDAAP from pg 3

A stand-alone UDAAP risk assessment is not required, but consideration should be incorporated in all risk assessments, such as Fair Lending, Product and Services Development, Vendor Management, and others unique to your institution.

Educate the team, and encourage them to speak up when something is confusing or unclear. Often those who are implementing strategy, marketing, lending programs, and policies are not doing so with malicious intent. It's similar to having someone else proofread a document. The writer of the document becomes blind at times to grammatical errors because of prolonged exposure to the words.

Create a policy, and take the time to educate the Board of Directors on potential red flags or areas most susceptible to UDAAP claims. Learn from others.

While several recent UDAAP consent orders were imposed on non-traditional lenders or "big banks," being attentive to these actions will only enhance your knowledge of how the regulators are thinking. Review your processes, looking for similarities to the accused. Avoid an "it can't happen to us" attitude.

Most importantly, ask the difficult questions around whether products, marketing, disclosures, lending, etc. could be perceived as harmful to consumers; and dedicate resources to a robust complaint management system to aid in the early detection of issues that could heighten UDAAP risk. Building a reputation and brand takes years of dedicated effort, and one UDAAP claim, even if disputable or unwarranted, can wreak havoc on all preceding success. Adjust them when necessary, but keep your UDAAP lens well-positioned and clear.

UBB Compliance, Katie Ferrell, Vice President, Senior Compliance Consultant • 601-522-9229 • katie.ferrell@ubb.com

UBB Welcomes

Kurt Cottier
Kurt started this past July as the Senior Vice President, and Senior Lending Officer. Kurt joined UBB with over 30 years of banking and lending experience.

Alan McLean
Alan started as Senior Vice President and Operations Director this past August. Alan brings over 20 years of banking experience to the UBB Operations Team.

Announcements

Mark Luukkonen
Congratulations to UBB's VP, Information Security Manager, Mark Luukkonen on 50 years in the banking industry. He was recognized as a Pioneer Banker by the Minnesota Bankers' Association, and Mark's 50 years of service were also recognized this past summer by BankIn Minnesota.

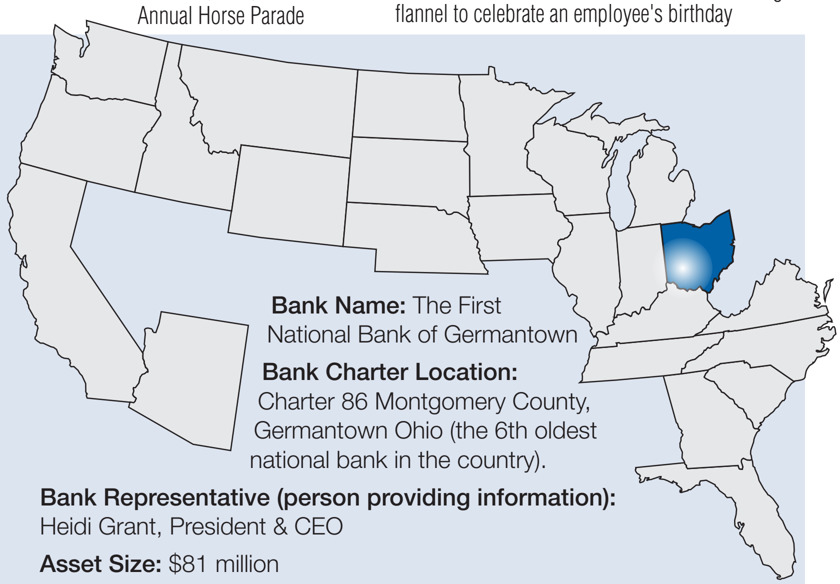
Keeping the *Community* in Community Banking

The First National Bank of Germantown • Germantown, Ohio

Just 15 miles Southwest of Dayton Ohio, in the picturesque Twin Creek Valley lies the city of Germantown. For over 150 years, The First National Bank of Germantown has taken a profound sense of ownership in the success of their community through their relationship building and community involvement. We sat down with Heidi Grant, President & CEO of The First National Bank of Germantown, to find out how they are *Keeping the Community in Community Banking*.

Heidi with Senior Lender, Tom, at the Annual Horse Parade

Staff of The First National Bank of Germantown wearing flannel to celebrate an employee's birthday



Bank Name: The First National Bank of Germantown

Bank Charter Location: Charter 86 Montgomery County, Germantown Ohio (the 6th oldest national bank in the country).

Bank Representative (person providing information): Heidi Grant, President & CEO

Asset Size: $81 million

Number of Locations: 1

Number of Employees: 15

Year Bank was Incorporated: September 19, 1863

City Population: 15,500

What is your community most known for?
Germantown is home to the Florentine, the 2nd oldest Inn in Ohio.

How is your bank involved in the community?
We sponsor numerous items through school organizations, from participating in retro basketball nights, to donating raffle items, and sponsoring gym floors. We also sponsor summer car shows and music for ladies' night. Our employees are members of several civic organizations, such as Rotary, Lion's Club, and the local Chamber of Commerce. Two of our employees are recipients of the prestigious Lion's Club Melvin Jones Award.

Do you have any goals or programs in place to encourage bank employees to be active in the community?
We ask employees to get involved and provide each one with 40 hours of paid volunteer time to encourage involvement.

What makes community involvement important to you and your bank?
We have been a thread in this community for over 159 years. The community is our family, and community involvement is just who we are and how we live.

What do you like best about your community?
How everyone comes together when others are in need. We have several families who have experienced tragedies, and this community comes together for them year after year. There is some serious love woven throughout this community.

Heidi and team cleaning up local disc golf course

Heidi and staff teach Jr. High students to manage money and budget

What do you like best about being a community banker?
Being personal with people and helping them open a new business, purchase their first car, or buy their first home or their dream home. I love answering the phone and helping a customer figure out their account or sponsoring the youth wrestling teams and little league. I love hearing a voice in the drive thru as I am passing by and stopping to chat while they wait on their transaction to be processed. It's just fun!

Turn Your Attention to Wire Fraud Prevention

By UBB Operations

Picture It: Stanley Jones, a long time bank customer approaches the teller line at your financial institution, some printed emails in hand and a sense of urgency written all over his face. Mr. Jones tells Sara, the young, newly hired teller, that he needs to send a wire transfer and it needs to be done quickly. Sara leans into her training and begins asking Mr. Jones some additional, clarifying questions regarding the nature of the wire. Mr. Jones gets more and more frustrated, finally blurting out, “My grandson is in trouble. Stop asking me questions, and help me get this done!”

As you read the scenario between Mr. Jones and Sara, red flags were likely popping up in your mind. Is Mr. Jones, the victim of an elder abuse scam? Could this situation be an email account compromise? Is Mr. Jones’s sense of urgency a tactic used by the scammers to get him to act quickly without considering the source of the request for funds? On top of the obvious business red flags, there are the complicating factors of customer dynamics. Is the customer always right? Sara is a young, newly hired teller and Mr. Jones has banked with you for years. Sara is unsure how far she should push Mr. Jones; she doesn’t want to make him upset or make him feel like she is questioning his integrity.

In the various payments channels available to consumers today, there are certain safeguards built in to prevent fraud from occurring. The debit and credit card industry has regulations, spending limits, behavioral anomaly detection software and authorization filters among the fraud prevention tools in their toolkit. Similarly, consumers who are sending funds via ACH are protected by NACHA rules and regulations, authorization requirements, transaction limits and more. Who or what is protecting consumers that want to send a wire transfer? We are! Financial service professionals are the FRONT LINE to prevent wire fraud.

There are several things we have a responsibility to do to help prevent fraudulent wire transactions from taking place, including: verifying account holder identity, identifying red flags and always reporting suspicious activity.

As fraudsters get more sophisticated, we must adapt our approach to verifying our customers’ identity. The old methods of relying on caller ID, the last four digits of an account holder’s social security number or even account history information aren’t enough anymore; this information could have already been compromised. We need to be more creative in the ways we verify identity by digging deeper and asking the questions that can’t be easily spoofed by fraudsters. Some ideas include: what’s your safety deposit box number, at which branch did you open your account, or after authenticating a caller or upon an in person visit, you could set-up an account password to use in lieu of verification questions.

Asking the “who, what, when, where, why” while initiating a wire transfer can uncover unusual behavior such as if someone is being taken advantage of or sending funds under other false pretenses. Looking for red flags can often help a fraudulent wire from being sent in the first place. Empowering your front line staff to ask questions about relationship details, the purpose of payment, or unusual account activity can head off a potentially devastating loss for the customer. If your staff suspects a wire may be fraudulent, make sure they know it is okay to refuse to send the wire or get the bank’s BSA or compliance officer involved.

Sometimes even with the best preventative measures in place, fraud can still happen. The quicker you can get word to the receiving bank that fraud has occurred the better. Follow your bank’s internal policies, file a suspicious activity report with FinCEN, encourage your customer to file a police report, and assure your customer that they are not in this situation alone.

To help prepare for what may be requested by the receiving financial institution, gather details and documentation regarding the fraudulent activity. This could include copies of your internal wire transfer request, a timeline of events, nature of the transaction, payment details and any law enforcement documents.

Fraud can happen at any financial institution at any time and unfortunately, sometimes we don’t think about enhancing procedures to identify fraud, until after it occurs. United Bankers’ Bank is committed to assisting your bank in any way possible to help mitigate fraud. We will be providing an upcoming Wire Fraud “Lunch and Learn” webinar. Please watch our website and your email for more information.

Disclaimer: This article is for informational use only. All statements contained herein are the sole opinion of the author.

UBB Operations • 800-558-6878

UBB Independent

United Bankers' Bank
Suite 1500
1650 West 82nd Street
Bloomington, MN 55431-1467

If you have questions about our products and services, please call us at **1-800-752-8140.**
www.ubb.com • Member FDIC

Friday, November 18th

UBB First for Your Success™