BANKERS' Hotline
THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXX, NUMBER 11 November 30, 2020

In This Issue

It's the Most Fraudulent Time of the Year!

by Teri Wesley

Seeing an increase in financial crimes and fraud during the holidays is par for the course in this industry. But as with nearly everything we've experienced this year, we can expect a "new normal" in seasonal fraud and scams. The coronavirus isn't the only thing hitting record numbers as it surges across the country and the world. The Federal Trade Commission (FTC) reports that more than 200,000 complaints of scams and fraud have been filed this year and Americans have lost more than $190 million to fraud related to the coronavirus. The FTC's Sentinel Network tracked about 206,000 reports of fraud, identity theft, spam telephone calls, and other potential COVID-related scams from January 1 through September 22.

Fraud is going even more viral on social media channels. According to the FTC's latest **Consumer Protection Data Spotlight** the number of complaints about scams that started on social media more than tripled in the last year. People reported losing more than $117 million to this type of scam in just the first six months of 2020, compared to $134 million for all of 2019. Online shopping topped the list of complaints from consumers who reported a scam to the FTC that originated on social media when they responded to an ad. Facebook and Instagram were the top two social media platforms identified in complaints by 94 percent of consumers. The surge in fraud is not just happening in the U.S. UK Finance reports over £27 million was lost to fraud at online marketplaces and auction websites in the first half of 2020.

While Black Friday has traditionally been the busiest shopping day of the year for big box stores and malls, people are playing it safe during the pandemic and doing their shopping online. A recent survey led by Pitney Bowes found that 57 percent of consumers plan to shop online more this year, with 45 percent reporting they already do more than half of their current shopping online – that's nearly three times the number pre-pandemic. Online shoppers are projected to spend a record $13 billion this year.

The pandemic has impacted how consumers live, work, play, and shop - and their financial safety. As transactions and distractions increase during the holiday, consumers become prime targets for seasonal scams and holiday hoaxes. These can lead to account takeovers, fraudulent activity, and identity fraud. According to an Experian survey, more than half (57%) of consumers feel the risk of identity theft is greater this year due to the pandemic. PYMNTS.com reported that over 60 percent of banks say fraud volumes are rising, with over 40 percent reporting that average fraud hit value is going up and that 22 percent of Americans have been targeted by pandemic-related fraud attempts since April.

Cybercriminals know that consumers are shopping online more and paying less attention to their bank and credit card statements during the pandemic, especially during the holidays. They also know that higher transaction volumes and a demand for faster processing times leave merchants vulnerable to attacks. With the increase in real-time payments, account push payment (APP) attacks have risen dramatically.

Fraudsters take advantage of the spending frenzy to hide their illicit transactions. Con artists prey on consumers who are looking for that too-good-to-pass-up bargain. It's not just online fraud and scams that become more prevalent this time of year. Other common holiday threats include phishing email scams, skimming devices at ATMs, retailer, and fuel stations, and gift card fraud. Counterfeit cases also rise as innovative new color printers that come out just before Christmas make it easier for creative crooks to create counterfeit checks or a passable IDs. Thieves will target ATMs under the assumption that banks keep more money in them for late night holiday shoppers.

(continued on next page)

It's the Most Fraudulent Time of the Year
(continued from first page)

During this most fraudulent time of the year, **staff training** and **consumer education** should be at the top of your holiday checklist. Train your frontline staff on how to detect fraudulent checks or fake IDs. Make sure they know the red flags that a consumer, particularly a senior customer, may be the victim of a scam. Have procedures and technology in place to identify unusual transaction activity on accounts. Increase robbery training and review opening and closing procedures. Be alert for mortgage and lending fraud that has substantionally increased during the pandemic.

Give the Gift of Education

While you're spreading holiday cheer on social media or your website, include the following tips to ensure your customers have a merry and bright holiday – and protect themselves from those nefarious cyber Grinches!

Think Before you Click. Never follow links in unsolicited emails. Check that any emails you receive are from a known or verified email address.

Authenticate and update. Use authentication methods offered by apps and websites, such as one-time passcodes sent via text or email or biometrics, particularly for banking and financial apps. Update passwords frequently and never reuse passwords.

Use trusted payment methods. New payment apps may be cool but they can also be bogus. Only use those you have verified are legitimate, such as PayPal or Zelle. If sending cash from your online or mobile banking app to a new recipient, do a small test transaction and confirm they got it.

Don't send anything via wire transfer or prepaid cards to someone you don't know. Use a credit card, single-use debit card, or prepaid reloadable card for online purchases.

When in doubt, hang up. Never provide credit card info as part of an unsolicited phone call. If it sounds too good to be true, it probably is.

'Tis the season for safe giving. To protect yourself from charity fraud, make sure the donation website is legitimate or an online request to support a person or family is someone you know or can be verified.

Monitor your accounts. Frequently check your financial accounts for any activity you do not recognize.

Monitor your credit report. Not just during the holidays. Periodically monitor your credit report for strange or unexpected activity for potential signs of identity theft.

The most wonderful time of the year is also the most vulnerable time of year for consumers struggling to make ends meet.

In The News

Regulatory Guidance on Operational Resilience

In recent years – and particularly this year – financial institutions have experienced significant challenges from a wide range of disruptive events, including technology-based failures, cyber incidents, natural disasters, and pandemics. These events, combined with a growing reliance on third-party service providers, highlight the importance for banks to strengthen their operational resilience. On October 30, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation issued interagency guidance in the form of sound practices that banks may use to strengthen and maintain their operational resilience. The "***Sound Practices to Strengthen Operational Resilience***" paper combines existing regulations and common industry standards to promote a comprehensive approach for effective governance, robust scenario analysis, secure and resilient information systems, and thorough surveillance and reporting.

The paper also includes an appendix focused on sound practices for cyber risk management and cybersecurity preparedness. The appendix is aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is "augmented to emphasize governance and third-party risk management." While the paper is directed at larger regulated banking organizations, it stresses the importance for firms of all sizes to review the paper and consider implementing those practices that are relevant to, and practical for, that institution. The regulators indicate that they intend to hold discussions in the coming months with the public to identify additional measures to improve operational resilience that may be incorporated into updates to the Guidance.

Google Branching Into Banking

Being the world's most popular search engine and email provider isn't enough for Google. The tech giant is continuing to make its move into the consumer financial services market. Google has redesigned Google Pay to add new financial management and loyalty features and to offer consumers checking and savings accounts from partner banks and credit unions. Google Pay recently expanded its availability and added 89 additional U.S. financial institutions, bringing its total to almost 3,000 supported banks and making it one of the most broadly supported mobile payment services available. While it has worked with most cards and large banks, this recent expansion includes smaller, regional banks and credit unions. The revamped Google Pay app includes new features that allow users to pay friends, track and manage budgets, and receive insights on their spending. With its expanded portfolio of partner banks, in 2021 users will have the option to open Google Plex checking and savings accounts through the app.

DOJ Blocking Fintech Monopolies

The U.S. Department of Justice (DOJ) is cracking down on potential fintech monopolies. Earlier this month when the DOJ discovered that payment card giant Visa was making a move to acquire fintech firm Plaid for $5.3 billion, the DOJ intervened with legal action to stop the merger. Visa already controls around 70 percent of the digital debit card payment market, from which it earned approximately $2 billion last year. While some apps are putting a dent in the digital transaction market, the DOJ asserts that buying Plaid would be an "insurance policy" to protect Visa's dominant market share.

The DOJ recently took issue with Intuit's planned acquisition of Credit Karma as well. The agency has ordered the fintech giant to sell Credit Karma's tax wing to Square before the acquisition so that Intuit (which also owns TurboTax) does not have the monopoly on all consumer tax software.

HSBC Launches Global Money Transfer Service

To compete with fintech money transfer providers Transferwise and Revolut, HSBC is launching a free mobile-based, real-time service for its customers to send funds in various currencies in over 20 markets without incurring any fees. With the bank's Global Money Account, customers can get instant access in a few clicks via their existing banking app. The service will launch in the U.S. and roll out to other markets in 2021. Instant international transfers to customers with other banks will be available in the future.

Statistics, Facts & Such

- Contactless payments are up due to COVID. Over 74% of Americans surveyed said they used their phone to order and pay for food and merchandise at least once a week, with nearly 48% using their phones for purchases several times a week or more. ***Mobile Payments Today, 11/12/20***

- More than half of Americans (54.8%) used their phone for online retail, 25% used it for food app/restaurant delivery and 9.3% used their phone for in-store purchase, such as "tap to pay" at checkout. ***Ibid.***

- During COVID-19, credit cards (55%) was the preferred method of payment versus mobile phone (16%), tap-to-pay cards (13%) and cash (12.5%). While 73% of Americans have paid for some merchandise, food, beverages or services with cash since COVID-19, 41% of Americans paid less frequently with cash during COVID-19. ***Ibid.***

- If contactless payments were offered through mobile ordering, self-service kiosks or tap-to-pay cards 49% of consumers would shop in-store. ***Ibid.***

- Once the pandemic is over, 77% of Americans said they will prefer to pay for merchandise, food, beverages and services with contactless payments. ***Ibid.***

- U.S. consumers generally rely on ATMs to fulfill their banking needs, and consumers are more than four times as likely to use their own bank's ATM (94%) as another bank's ATM. ***ATM Marketplace, 11/20/20***

- More than half of 18-34 year olds using Buy Now Pay Later (BNPL) have missed a payment and nearly two thirds (62%) say BNPL is making them spend more. ***Finextra, 11/27/20***

- Over half of consumers surveyed want BNPL products to be regulated, while 52% want providers to consider their credit history before financing is approved. ***Ibid.***

- Nearly half (45%) of those surveyed would like BNPL to be integrated with their current account or credit card. ***Ibid.***

Tech Update

Smart Lockers for Safer Banking

With the surge in COVID cases and shutdowns and quarantines still in place in many parts of the country, financial institutions are exploring ways they can safely and securely serve their customers – and keep their employees safe. Branch and digital transformation solutions provider FTSI has launched a contactless delivery solution for banks, credit unions, and beyond.

FTSI's Smart Lockers for Banking can be integrated within the branch location, outside the branch or at a hub location. Customers receive access codes from the bank, which are used to track and maintain audit trails when customers retrieve their items from the locker. The smart lockers provide a safe, secure means for:

- Consumer Pickup and Drop off
- Debit cards
- Cashier's checks
- Coin orders
- Document Exchange

Smart Lockers for Banking can be integrated at branch locations either indoors, outdoors, or at other places convenient to where customers live or conduct daily errands, notes company founder and CEO Susan Napier. "*We developed Smart Lockers for Banking as a way for our clients to deliver superior customer experiences and convenience while also allowing branches to extend hours of availability and to gain operational efficiencies. Now, with COVID-19 compelling physical distancing through the foreseeable future, financial and other enterprises with similar needs have even greater incentives to explore this exciting new self-service capability.*"

Benefits and Features:

- No contact delivery solution
- Extended hours of availability
- Full reporting capabilities
- Smart Locking Device
- Embedded intelligence and
- Integrated sensing
- Fully configurable for different size and space requirements
- Suitable for indoor and outdoor applications.

For more information, go to https://ftsius.com/smart-lockers/

Spotlight on What's Happening

ACAMS
Anti-Financial Crime
Virtual - Hot Topics
February 25, 2020
Info: (305) 373-0020
www.acams.org

BANKERSONLINE
2021 BSA/AML Conference
March 2-3, 2021
www.bolconferences.com
BSA and OFAC 2021 10 Hot Topics
Webinar, January 20, 2021
www.bollearningconnect.com
Info: (888) 229-8872, ext 87

Regulatory Deadlines

Comments due on FTC Prescreen Opt-Out Notice Rule Proposal
due December 7, 2020

Comments on OCC 'Fair Access to Financial Services' proposed rule
due January 4, 2021

Training Page

Essential Workers at Increased Risk of Suicide During the Pandemic

by Jim Beveridge

Suicide, according to the National Institute of Mental Health (NIMH), is a significant public health problem and a leading cause of death in the United States. The effects of suicide go beyond the individual who takes their own life: it can have a devastating and long-lasting impact on family, friends, and communities.

On September 10, 2020, the Pan American Health Organization (PAHO) suggested that the COVID-19 pandemic may increase suicide risk factors. The Mayo Clinic agrees, warning that during the pandemic, "you may experience anxiety, fear, fru*stration, sadness, and loneliness – to the point that those feelings become constant and overwhelming*."

Essential Workers

The hardest-hit demographics, according to a recent study by the Centers for Disease Control and Prevention (CDC), are essential workers. 21.7% of Essential Workers surveyed by the CDC expressed having seriously considered suicide in the past 30 days. Symptoms of pandemic-related stress, along with increases in substance abuse, were also more prevalent among essential workers than other workers.

Banking employees that are considered essential workers are at an increased psychological risk because their jobs require close contact with the general public and coworkers. Many bank personnel are not only fearful about contracting the virus themselves. They are also concerned about bringing COVID-19 home to their family members, especially those with underlying medical conditions or other high-risk factors.

The British Medical Journal (BMJ) reports that "studies modeling the effect of COVID-19 on suicide rates predicted increases ranging from 1% to 145%." The BMJ urges caution and notes that peer-reviewed academic studies for higher-income nations like the United States suggest no rise in suicide rates, and even a fall in the early months of the pandemic. However, the authors contend that we must remain alert to emerging risk factors for suicide and ensure that the appropriate services are made available for people in crisis.

David Puder, MD, a psychiatrist at Loma Linda University Behavioral Health, recommends six tips for front-line, essential workers:

- Getting enough good sleep
- Exercising daily
- Getting away to places that allow one to distance themselves from stressors.
- Keeping in touch by phone with friends and loved ones
- Maintaining a healthy diet.
- Engaging with a mental health professional

Warning Signs

The warning signs of suicidal thoughts, according to the National Institute for Mental Health, may include:

- Talking about:
  - Wanting to die
  - Great guilt or shame
  - Being a burden to others
- Feeling:
  - Empty, hopeless, trapped, or having no reason to live
  - Extremely sad, more anxious, agitated, or full of rage
  - Unbearable emotional or physical pain
- Changing behavior, such as:
  - Making a plan or researching ways to die
  - Withdrawing from friends, saying goodbye, giving away essential items, or making a will
  - Taking dangerous risks such as driving extremely fast

Reaching out for help: The Mayo Clinic recommends getting help right away if you think that you may hurt yourself or attempt suicide by taking any of the following actions:

- Contact your doctor or mental health professional.
- Call a mental health crisis number or a suicide hotline. In the U.S., call the National Suicide Prevention Lifeline at 1-800-273-8255 any time of day — press "1" to reach the Veterans Crisis Line or use Lifeline Chat.
- Call 911 or another local emergency number.
- Reach out to a close friend or loved one.
- Contact a minister, spiritual leader, or someone else in your faith community.

If someone else says that they are thinking of suicide or behaves in a way that makes you think the person may be suicidal, the Mayo Clinic advises that you not ignore or play down the situation. If you're concerned, consider these actions:

- Offer the person the opportunity to talk about their feelings, but keep in mind that it's not your job to substitute for a mental health professional.
- Encourage the person to seek professional treatment or call a mental health crisis center or suicide hotline.
- Urge them to seek help from a trusted person, support group, or faith community.
- Offer to help the person find the necessary assistance and support.

If someone is posting suicidal messages on social media, many sites, such as Facebook or Instagram, offer options on how to respond — search the site for "suicide" or "suicide prevention." In urgent situations, call 911 or the National Suicide Prevention Lifeline at 1-800-273-8255 for help.

It is important to remember that we are not responsible for preventing someone from taking their own life. However, our support and intervention may help the person see that other options are available to stay safe and get treatment.

For additional information: Visit the Mayo Clinic website for "COVID-29 and the Risk of Suicide" at https://www.mayoclinic.org/diseases-conditions/coronavirus/in-depth/covid-19-suicide-risk/art-20490350.

Or download a copy of "Suicide in America," a fact sheet developed by the National Institute of Mental Health https://www.nimh.nih.gov/health/publications/suicide-faq/tr18-6389-suicideinamerica-faq_149986.pdf.

Proposed Change to BSA Reporting Threshold

To help identify and prosecute bad actors who are using smaller value cross-border wire transfers to facilitate financial crime and other illicit activity, the Federal Reserve and FinCEN published a joint notice of proposed rulemaking to reporting guidelines for international transactions. The agencies are seeking feedback on the proposed change that would lower the threshold for reporting international transactions from $3,000 to $250. The agencies said that increased recordkeeping and reporting concerning these transactions would be valuable to law enforcement and national security authorities. This would help law enforcement and regulators detect, investigate and prosecute financial crimes by maintaining a paper trail about persons sending and receiving funds through the funds transfer system, said the agencies.

The rule only applies to international money transfers. The threshold for domestic transactions would remain unchanged at $3,000. In the notice of proposed rulemaking, the agencies also proposed to clarify that the rules also apply to virtual currency and digital assets that have legal tender status.

Crypto and Green ATMs

ATMs have come a long way since the first ATM in the U.S. debuted and dispensed cash to customers at Chemical Bank in Rockville Centre, New York on September 2, 1969. In 2013, the first-ever Bitcoin ATM by Robocoin was placed in a coffee shop in Vancouver. Allowing customers to trade Bitcoin for cash, and vice versa the machine saw $10,000 in BTC transacted on its first day. Today, the estimated number of crypto ATMs around the world that allow customers to buy and sell Bitcoin and other altcoins for cash is about 11,665 (an 80% increase from 2019).

Earlier this month, Bank of America installed the nation's first solar-powered remote ATM in Woodbridge, Virginia. It's the first of three solar-powered stand-alone ATMs the bank plans to bring online before the end of the year as part of their Onsite Solar Initiative to incorporate solar power into the design standards for all its remote ATMs. BoA also plans to install more than 60 solar panel installations across its entire operations, including financial centers, ATMs, office locations and other operational buildings.

Focus on Fraud

A Swift Update on Cyber Threats

The global pandemic has forced many businesses, including financial firms, to operate remotely and increasingly depend on digital processes, leading to increased risks of cyber attacks. At a two-day Swift Community Update virtual event held earlier this month, one of the sessions focused primarily on cyber threats targeting the financial sector. One of the most notable factors highlighted in the session was that, despite technological advancements in security, the easiest criminals gain access to a bank's network remains via the human element – most commonly through an email compromise. Money mules are also still an integral part of a fraudster plans to cover their tracks and cash out following successful attacks. "*Money mules act as an effective intermediary between the initial cyber attack and the onward transfer of the funds to the criminal and threat groups behind these attacks*," said Simon Viney, cybersecurity financial services sector lead at BAE Systems. "*They help to obfuscate the chain of events in the money trail.*"

The following payment fraud trends that have been observed by Swift were also highlighted and discussed:

- Attackers targeting banks which process a low amount of cross-border payments and are based in countries with a high or very high risk rating on the Basel AML Country Corruption List. For example, regions such as Africa, South East Asia and Latin America
- The amounts sent in individual fraudulent transactions have significantly reduced, from tens of millions of US dollars, to between 250,000 and two million US dollars
- Attackers historically would have issued fraudulent payments outside of working hours, but this is now more likely to occur during working hours.

ATM Cyber Threats

Cyber attacks targeting ATMs and central servers that control ATMs are increasingly leading to the theft of personal data, account numbers, and PINs. Since these types of attacks require the thieves to take further actions to convert the data into money, ATM jackpotting attacks are even more popular wiyh ATM cybercriminals. By exploiting the physical and/or software-based vulnerabilities of an ATM, they can gain immediate access to cash directly from the targeted ATM. In the last five years, global financial organizations have lost millions to jackpotting attacks. Global banking software solutions provider Auriga has published a white paper titled ***The Current State of Cybersecurity for ATMs*** available for download free at https://www.aurigaspa.com/en/resources/white-papers/. Earlier this year, the company acquired Lookwise Device Manager (LDM), a cyber security platform that offers a comprehensive set of functionalities to protect, monitor and control ATM equipment. LDM provides real-time visibility into the hardware, software and users to help stop current and future threats.

A Cyber Risk Assessment Tool for Banks

Mastercard is lending a helping hand to banks in the fight against cyber threats. According to the credit card giant, at least 1 in 4 organizations have experienced a cyber attack in the last 12 months. Attacks are being further exacerbated by the coronavirus pandemic, as criminals have been quick to capitalize on the chaotic situation caused the health crisis, with many banks suffering from stolen assets or compromises in security in recent months.

The global payments provider has launched an AI-powered suite of tools for banks to assess cyber risk across their ecosystem and prevent potential breaches. Mastercard's Cyber Secure solution enables banks to continuously monitor and track their cyber posture to identity potential threats and weaknesses within their operations. It helps to reduce financial losses associated with attacks, saves time and resources, and provides a comprehensive view of cyber risk through one application. Banks can also help merchants understand their own cyber risk, preventing hundreds of millions of dollars in potential fraud. The risk assessment is performed using advanced AI that combines multiple public and proprietary data sources and evaluates the data against 40 security and infrastructure criteria. Each vulnerability is analyzed to produce a cyber risk rating and issue priority navigator.

From the Editor

Gratitude: Essential for Effective Leadership

by Jim Beveridge

Confidence, strength, integrity, passion, and persuasion are the character traits that many people think of when describing great leaders. One attribute that rarely makes any list is gratitude. Why gratitude, and why would it be considered essential for effective leadership?

An extensive body of research has revealed the tremendous influence of gratitude in every aspect of life. Robert A. Emmons, Ph.D., at the University of California at Davis, conducted a wide-ranging study of the impact of gratitude on one's overall well-being. Emmons concluded that the expression of gratitude has a profound and positive effect on our health, moods, and even our marriage's survival. Another study at Northeastern University conducted by Monica Y. Bartlett, Ph.D. and David DeSteno, Ph.D., concluded that gratitude drives helping behavior, increases assistance provided to strangers, and improves relationships.

Geoffrey James, author, journalist, and contributing editor at In.com, wrote, "*If you're not exercising this emotional muscle, you're probably setting yourself up for failure. I'm utterly convinced that the key to lifelong success is the regular exercise of a single emotional muscle: gratitude.*" Gratitude, then, is not just an emotion but an entire approach to life that requires intentionality.

Daniel Threlfall, in an article titled "Gratitude: The Leader's Most Underused but Powerful Tool," for teamgantt.com, provides a compelling case for why gratitude is a must for effective leaders. Threlfall contends that since appreciation is such an important behavior, it can revolutionize one's leadership. Gratitude demands a response, and that response is invariably positive.

A leader who is grateful towards their employees gains their respect: The simple act of gratitude produces other behaviors. Anytime that a leader intentionally thanks their employees, respect is earned. Because gratitude is a virtue, we tend to admire those who exemplify it.

A leader who thanks their employees gains their trust: People cannot fake gratitude, which is one of the primary reasons it is one of the emotions that elicits trust. Consider the work relationship where a boss tells an employee," I am thankful for the effort you put into that report. It was exceptional and provided the appropriate level of details to present to our client." The employee who received that feedback is not concerned about losing their job. Instead, they are thinking, "I trust my manager."

A leader who thanks their employees gains their appreciation: All of the research indicates that gratitude is one of the pinnacles of virtue. We appreciate this goodness in others – thus, when a leader expresses gratitude towards other people, our behavior is appreciated.

A leader who expresses gratitude prevents other undesirable emotions: Threlfall suggests that grateful people are rarely angry and angry people are rarely grateful. Gratitude neutralizes anger and jealousy and can abolish some of the malice's too often associated with poor leadership, such as micro-management, authoritarianism, rudeness, and more.

One's gratitude must have an ultimate objective. It is challenging to be grateful for nothing or to have it in a vacuum. Genuine appreciation, by its very nature, has a purpose and cannot be faked. One may be able to pretend grateful a few times, but it will not work unless you are deeply and sincerely thankful. The research indicates that we can improve and expand those muscles by intentionally and regularly exercising gratitude and cultivating genuine appreciation. The downside of the Thanksgiving holiday is that it only comes around once a year. An appropriate level of gratitude expresses it frequently – gratitude is a daily effort. If one takes the time to think about the subject, there are many things to be grateful for. The secret is that you need to think about it – frequently.

Gratitude is meaningless unless it is specific. You have to be thankful for something. Here are a couple examples of specificity:

> "*Thank you for sending me that email last night. I know that you worked late to put the material together, and it was precisely what I needed for my meeting this morning. Thanks again for your hard work and the detailed information.*"
>
> "*I appreciate the way you handled that tense situation with that customer this afternoon. You spoke softly, in a controlled manner, and effectively de-escalated the customer's anger and frustration. Great job.*"

People enjoy talking about good leadership character traits as if somehow, we could codify the attributes in a comprehensive list. However, every list can be different. For one reason or another, gratitude seldom makes anyone's list. Try a little appreciation and see what happens – you may be pleasantly surprised at the results.

War Stories

Mask Required

In today's unprecedented times, instead of asking visitors to remove face coverings, bank staff are telling them to put them on. When a man believed to be in his late 30s or 40s entered a Chase bank branch in Fallbrook, CA not wearing a mask – which was required to prevent the spread of COVID – bank staff informed him that he needed to wear mask to receive service. The man left the bank and returned later wearing a mask. He walked to a counter in the middle of the lobby, where he wrote out a demand note on a deposit slip, which he passed to a teller – with his mask on. "Don't make any sudden movements," it read in part. "Just read the note." Now it was the teller's turn to comply, who handed the man his cash, and he left the bank. The suspect, who had a noticeable limp and wore a black hooded sweatshirt and sweatpants, black baseball hat, black sunglasses, and black mask has not yet been identified – even though surveillance cameras caught a clear photo before he masked up.

Quit While You're Ahead

A 19-year-old man who robbed a Coasthills Credit Union in Lompoc, CA, after slipping the teller a note and fleeing with an undisclosed amount of cash should have quit while he was ahead. Instead he decided to try his luck a second time at Mechanics Bank in Guadalupe. He left that bank without any cash. Witnesses provided a description of the man and his vehicle who was later arrested following a high-speed chase. The description of the suspect and the vehicle (which was stolen) was shared with neighboring law enforcement and led to his subsequent second arrest by the Lompoc Police Department for the earlier credit union robbery.

Came Prepared

When Aaron Honaker, a Coral Gables attorney, decided to switch careers to bank robbery, he thought of everything. On his fourth job, he had instructions, he cased the bank, and he had a carefully crafted demand note. Honaker was arrested when he attempted to rob a TD Bank branch. When the prepared thief was later found in a parking garage, he had multiple folded demand notes, a notebook with instructions on how to rob banks, and a hammer which he told police was "to escape any glass mantraps trigged by bank security." Honaker has been charged with two counts of bank robbery and four counts of attempted bank robbery. Hope he's prepared for where he'll be spending the next few years.

Questions & Answers

Question: What exactly is a conversion loan?

Answer: A legitimate conversion loan is a loan that rolls over, or converts, to a new structure after a specified term. Pricing both segments allows the parties to account for the sequential closing and funding dates. This functionality enabled at the product level is often used to price construction-to-permanent loans, where a short-term loan converts to permanent financing at a later date.

Conversion loans can be found in construction scenarios; they, can also be utilized to create other legitimate financing structures such as a line of credit converting to a fixed-term or installment loan. Lenders may also set up conversion options on other commercial loan products.

Another example, according to Investopedia.com, is asset-conversion loans. These short-term loans are typically repaid by liquidating an asset. Bankrate.com notes that an asset-conversion loan is issued to a company that needs an immediate infusion of cash to meet its current financial obligations. The collateral put up to pay back the loan is usually inventory, accounts receivable, or other assets directly related to the business' day-to-day operations. Asset-conversion loans are sometimes used by companies with highly seasonal businesses, such as retailers that earn most of their revenue around Christmas.

Conversion loan frauds. Conversion loan frauds can be problematic for financial institutions and consumers. For example, a conversion auto loan fraud involves a secured car loan that converts into an unsecured loan when the lender never receives title to the vehicle. In August 2019, a team of fraudsters cheated banks and credit unions by filing paperwork for loans on vehicles that did not exist. According to the US Attorney's Office for the Northern District of Georgia, the scheme sought over 80 auto loans, attempting $2.7 million in fraud and resulting in losses totaling $1.7 million before the seven scammers were caught.

Fraudulent activity relating to Home Equity Conversion Loans (HECM loans) target senior citizens and other consumers. Reverse mortgage and HECM scams can be engineered to trick borrowers into signing away the equity in their homes. In contrast, other scams are designed to help fraudsters profit by illegally taking the equity built up in a renovated or "flipped" property. Victims of these schemes are usually offered a too-good-to-pass-up investment opportunity or refinancing opportunity. There are two fundamental ways that borrowers can protect themselves from these schemes:

- Ignore any unsolicited offers connected to HECM loans, reverse mortgages, and other loans.
- Seek FHA-approved lenders for any FHA reverse mortgage product.

Question: Do you recommend the use of "Simulated," "Dummy," or "Fake" surveillance cameras to augment genuine camera placements? Manufacturers and distributors of these non-functioning devices suggest installing one or more of these cameras is one of the best ways to provide security and reduce costs. Their marketing material suggests that dummy cameras can help deter crime when appropriately utilized with real equipment. For example:

- The appearance of security can be enough to scare off criminals and having some deterrence is better than having none at all.
- Fake cameras do not require circuitry or connections and can be installed virtually anywhere.
- The dummy cameras will deter inexperienced, low-level criminals.

Answer: A fake or dummy security camera is a non-functioning device designed to appear like a real closed-circuit television camera. It is often used as a deterrent in less vulnerable areas. Fake cameras are generally deployed as a mere psychological means to prevent criminal behavior.

The Federal Deposit Insurance Corporation (FDIC) and the National Credit Union Administration (NCUA) both require that financial institutions maintain active security camera systems. However, the regulators have not provided specific guidelines about the requirements for those surveillance systems.

We recognize that banks and credit unions still experience crime inside and outside their facilities despite the extensive use of security cameras. However, we do not recommend using a dummy or fake surveillance cameras by financial institutions in any capacity. We also strongly recommend that inoperative cameras be repaired or replaced as soon as possible.

Our recommendations are based on several factors.

Unconvincing visual appearances. Seasoned criminals will generally be able to identify fake surveillance cameras, despite blinking LED lights.

Dummy cameras can create a "False Sense of Security." Suppose a customer or staff member is attacked outside your bank or in a parking lot "secured" by a dummy camera. In that case, they may be able to argue in court that they relied on the false sense of security offered by the purported video surveillance. This reliance on false protection could lead to financial liability for the financial institution.

Additional legal risks and implications. Closed Circuit Television (CCTV) installations abide by strict laws and regulations, and real or fake cameras must adhere to those rules.

In conclusion. Banks and credit unions are generally heavily-protected businesses with physical security measures, including vaults, alarms, guards, and bullet resistant barriers. The CCTV surveillance systems are the backbone of the financial institution's security program. They serve as a layer of deterrence and provide a virtual record of almost everything happening within and outside the facility. Prominently placed cameras covering doors, exits, teller windows, and other spaces remind potential robbers, burglars, and fraudsters that they are being watched and recorded. Undermining the value of the CCTV surveillance system with non-functioning dummy cameras is both counterproductive and risky.

Got a Question?

Simply send your question to bh@bankersonline.com and we will do our best to help. And you may see it reprinted on this page — anonymized, of course!

Got a Question? *We're here to help! Submit your questions to us via email at* ***bh@bankersonline.com***

What do OTHER BANKERS do?

Helping Those Help Others

During these unprecedented times, consumers and businesses are in need of financial and other assistance more than ever before. To help the local organizations in their region supply those needs, **Franklin Savings Bank** in Franklin, NH has awarded $39,700 to ten nonprofit groups. The grants were awarded to through the FSB Fund for Community Advancement, the philanthropic arm of the bank. Catholic Charities of NH, Grafton County Senior Citizens Council, Inc. (Bristol), and Health First Family Care Center (Franklin) were among the recipients of the grants. Established in 1997, to date the Fund has awarded 225 grants totaling $1,029,807 to support a broad range of community activities. Since 2009, FSB has donated over 11 percent of its net income to charity.

A Month of Giving

Nursing homes and long-term care facilities have been some of the hardest hit by the COVID pandemic. In Illinois, **Washington Savings Bank** is fulfilling wish lists of 16 local nursing homes, assisted living, and memory care facilities in the Effingham and Mattoon areas. The bank kicked off a new #MonthofGiving campaign on November 1st. Items that were dropped off by local residents or donated by employees to give to residents of these facilities included tablets, CD players with CDs, DVD players with movies, bird feeders, activity books, crafts, snacks and personal hygiene items. The bank also gave back to their customers through daily drawings during the month of November for a daily Thanksgiving turkey, $100.00 donation to the charity of their choice, and a gift card to a local restaurant. In addition, the bank provided monetary donations to many local charitable organizations.

Virtual Bingo Fundraiser

With traditional fundraising efforts not possible this year due to social distancing measures to prevent the spread of COVID, one financial institution is getting creative with their Giving Tuesday fundraiser. The Center for Financial Empowerment (CFE), the nonprofit founded by **SCE Credit Union**, is holding a virtual Bingo Bash fundraiser on Giving Tuesday, December 1. Games will be played online via Zoom. Proceeds collected from the purchase of bingo cards ($25 for single player, $100 for four-pack player cards) benefit the CFE to help fund the delivery of its Financial Capability Program courses to 1,500 high school students at Basic Academy in 2021.

Donating Dough

While making Christmas cookies out of your favorite dough is a popular tradition, a credit union in Oregon is collecting dough to help local residents in need. **Mid Oregon Credit Union** is holding its annual Holiday Dough Fundraiser that supports local charities that provide food, clothing, and shelter for individuals and families in the greatest need during the holidays. Members and the general public drop off their Holiday Dough donation by cash or check – or for a safer option the bank has a convenient online form for submitting contactless donations. One hundred percent of the donations will benefit designated local food banks and agencies. Last year, credit union members and the community contributed nearly $3500 to local holiday food bank through the campaign.

And in CONCLUSION

"You caught a virus from your computer and we had to erase your brain. I hope you've got a back-up copy!"

PURPOSE:

TO keep front line, security, and operations personnel up-to-date on industry trends, regulatory and compliance issues and industry related techniques. To assist administrators in maintaining high morale. To provide a timely, reliable information source for the banker who does not have access to all pertinent banking publications, nor the time to read and evaluate them. To supply a sounding board for the purpose of sharing information and creating communication between all parts of the financial industry. To assemble all of the above in a read-able, understandable, usable format that can be photocopied and distributed in-house by each subscriber.

PUBLISHER
George B. Milner, Jr.
Bankers Information Network

BANKERS' Hotline

EDITOR
Jim Beveridge
Bankers' Hotline

(ISSN 1046-1728) published 12 times a year by Bankers' Hotline, PO Box 1632, Doylestown, PA 18901, $299/year. Subscription orders, renewals and Letters to the Editor may be sent to the same address or emailed to bh@BankersOnline.com.