BLR MANAGEMENT CONSULTING, INC.

NEWSLETTER

PARTNERS IN BUSINESS - OUR APPROACH IS SIMPLE...PARTNERSHIP IN BUSINESS, QUALITY IN PRODUCT AND INTEGRITY IN PEOPLE

10 Scams Targeting Bank Customers By FDIC Consumer News

The basics on how to protect your personal information and your money:

The FDIC often hears from bank customers who believe they may be the victims of financial fraud or theft, and our staff members provide information on where and how to report suspicious activity. To help further, **FDIC Consumer News** includes crime prevention tips in practically every issue. As part of that coverage, we feature here a list of 10 scams that you should be aware of, plus key defenses to remember.

1. **Government "imposter" frauds:** These schemes often start with a phone call, a letter, an email, a text message or a fax supposedly from a government agency, requiring an upfront payment or personal financial information, such as Social Security or bank account numbers. "They might tell you that you owe taxes or fines or that you have an unpaid debt. They might even threaten you with a lawsuit or arrest if you don't pay," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "Remember that if you provide personal information it can be used to commit fraud or be sold to identity thieves. Also, federal government agencies won't ask you to send money for prizes or unpaid loans, and they won't ask you to wire money to pay for anything."
2. **Debt collection scams:** Be on the lookout for fraudsters posing as debt collectors or law enforcement officials attempting to collect a debt that you don't really owe. Red flags include a caller who won't provide written proof of the debt you supposedly owe or who threatens you with arrest or violence for not paying.
3. **Fraudulent job offers:** Criminals pose online or in classified advertisements as employers or recruiters offering enticing

Inside this issue

opportunities, such as working from home. But if you're required to pay money in advance to "help secure the job" or you must provide a great deal of personal financial information for a "background check," those are red flags of a potential fraud. Another variation on this scam involves fake offers of part-time jobs as "mystery shoppers," who are people paid to visit retail locations and then submit confidential reports about the experience. In an example of the fraudulent version, your job might be to receive a $500 check, go "undercover" to your bank, deposit the check into your account there, and then report back about the service provided. But you also would be instructed to immediately wire your new "employer" $500 out of your bank account to cover the check you just deposited. Days later, the bank will inform you that the check you deposited is counterfeit and you just lost $500 to thieves. One warning sign of this type of scam is that the potential employer requires you to have a bank account.

4. **"Phishing" emails:** Scam artists send emails pretending to be from banks, popular merchants or other known entities, and they ask for personal information such as bank account numbers, Social Security numbers, dates of birth and other valuable details. The emails usually look legitimate because they include graphics copied from authentic websites and messages that appear valid.

"We have also seen emails with links to fake websites that are exact copies of real websites for FDIC-insured banks, except the web addresses are slightly different than the real ones," said Doreen Eberley, director of the FDIC's Division of Risk Management Supervision, which is in charge of the agency's policies and programs related to financial crimes. "These sites are used to trick people into giving up valuable personal information that can be used to commit identity theft."

5. **Mortgage foreclosure rescue scams:** Today, many homeowners who are struggling financially and risk losing their homes may be vulnerable to false promises to refinance a mortgage under better terms or rates. But borrowers should always be on the lookout for scammers who falsely claim to be lenders, loan servicers, financial counselors, mortgage consultants, loan brokers or representatives of government agencies who can help avoid a mortgage foreclosure and offer a great deal at the same time. These criminals will present homeowners with what sounds like the life-saving offer they need. Instead, the homeowner is required to pay significant upfront fees or, even worse, tricked into signing documents that, in the fine print, transfer the ownership of the property to the criminal involved. Common warning signs of fraudulent mortgage assistance offers include a "guarantee" that foreclosure will be avoided and pressure to act fast.

6. **Lottery scams:** You might be told you won a lottery (typically one that you never entered) and asked to first send money to the "lottery company" to cover certain taxes and fees. Similar examples involve bogus prize winnings and sweepstakes. "In one example, a scammer sent a letter to people using falsified FBI and FDIC letterhead telling them they won a popular, well-known lottery but that they needed to send money by wire transfer to a lottery 'official' in order to secure the winnings," Benardo said. "The 'official' was really a crook hoping to trick people into sending money."
7. **Elder frauds:** Thieves sometimes target older adults to try to cheat them out of some of their life savings. For example, telemarketing scams may involve sales of bogus products and services that will never be delivered. Warning signs include unsolicited phone calls asking for a large amount of money before receiving the goods or services, and special offers for senior citizens that seem too good to be true, like an investment "guaranteeing" a very high return. To help seniors and their caregivers avoid financial exploitation, the FDIC and the Consumer Financial Protection Bureau have developed Money Smart for Older Adults, a curriculum with information and resources (see our News Briefs).
8. **Overpayment scams:** This popular scam starts when a stranger sends a consumer or a business a check for something, such as an item being sold on the internet, but the check is for far more than the agreed-upon sales price. The scammer then tells the consumer to deposit the check and wire the difference to someone else who is supposedly owed money by the same check writer. In a few days, the check is discovered to be a counterfeit, and the depositor may be held responsible for any money wired out of the bank account. Victims may end up owing thousands of dollars to the financial institution that wired the money, and sometimes they've also sent the merchandise to the fraud artists, too.

9. **"Ransomware":** This term refers to malicious software that holds a computer, smartphone or other device hostage by restricting access until a ransom is paid. The most common way ransomware and other malicious software spreads is when someone clicks on an infected email attachment or a link in an email that leads to a contaminated file or website. Malware also can spread across a network of linked computers or be passed around on a contaminated storage device, such as a thumb drive.
10. **Jury duty scams:** A thief makes phone calls pretending to be a law enforcement official warning innocent people that they failed to appear for jury duty and threating an arrest unless a "fine" is paid immediately. And to pay up, the caller asks for debit account and PIN numbers, allowing the perpetrator to create a fake debit card and drain the account

To learn more about how to avoid financial scams, search by topic in back issues of **FDIC Consumer News** and the FDIC's multimedia presentation Don't Be an Online Victim. Also find tips from the interagency Financial Fraud Enforcement Task Force.

Press Releases & Thought Leadership

Thank you for turning to RLR for the latest in industry news! The banking and payments landscape is changing everyday – for the very latest, please follow us on Twitter and LinkedIn. To learn more about how RLR can help you, stop by our website at https://rlrmgmt.com.

A Snapshot of our Webinars & Workshops!

RLR has developed a series of **complimentary** educational webinars and workshops. We highlight a variety of topics and discuss hot button issues with our current and prospective clients. These webinars and workshops provide insight as well as facilitate discussions among the attendees to encourage knowledge sharing.

RLR recently hosted a webinar on May 17, 2017, where Tom Frale, Director of Business Development presented the following:

- Changes in Digital Payments Landscape, Is Your Institution Ready?

RLR recently hosted a workshop in Ontario, CA on April 5th, 2017. Ruth Razook presented the following topics:

- Current Expected Credit Losses (CECL)
- ADA Compliance: Is Your Website Accessible?

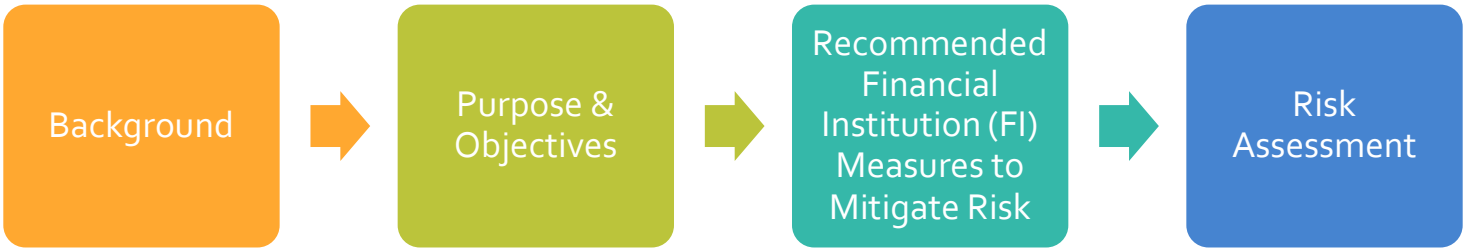
Diana Strade presented the following topic:

- BSA: Regulatory Hot Buttons & Best Practices for your Compliance Program

RLR Technology Guidance Program

For the past twenty years, RLR Management Consulting has had a program that we call our **Technology Guidance Program**. This program was initiated to assist our clients with understanding the latest regulatory guidance updates that are periodically released. We review the guidance in detail and structure an easy to understand Toolkit that summarizes the guidance, what the impact on the bank will likely be, and defines the actions the bank needs to take, including risk mitigation activities, to adhere to the new guidance.

As part of our **Technology Guidance Program**, our Toolkits outline the following for each FIL released:



Our Toolkits may continue with discussing Contracts, On-going Oversight, Contingency, Event Planning, and Emerging Risks. This is a general format we publish for most newly published guidance. Our summaries are published within 30 days of the published guidance.

Our Tech guidance program is offered to our clients on an annual subscription basis. Cost of the annual subscription is $1,500, payable in January of each year.

For more information or to enroll in the program **CLICK HERE!**

Shielding Your Institution's Brand from Toxic Online Content

The subject of brand safety isn't something new or unique to digital. For decades, brand managers kept their commercials out of violent TV shows or away from channels that present risqué content. The same idea holds true in digital. However, in TV there are a finite number of channels and shows that an advertiser needs to evaluate. But when you use online programmatic media buying platforms, there are billions of opportunities to buy an impression. This makes it much more challenging to monitor the placement of advertisements, and do so in real time.

While marketers will never have 100% oversight or control over the adjacent context of their ads — online or off — there are a few tools that marketers can utilize to address brand safety concerns, each with its own unique benefits and challenges. (To read the full article click here)

Technology Corner by Northstar Technologies

Are You Ready for Disaster Recovery in The Cloud?

The climate of regulatory compliance surrounding disaster recovery and business resumption has left many IT managers scratching their heads. From what scenarios must your IT infrastructure be recoverable? What should your RTO be? Can you recover from a regional pandemic event? Is your DR plan great on paper, but can you effectively implement it and test it? How much money can I spend before the cure is worse than the disease? Who can help me navigate this?

The answer is in the cloud.

The cloud has become an enabling technology that has allowed smaller companies with limited resources, the capability to implement disaster recovery technologies that were up until recently accessible only to large companies. By engaging a technology partner that has the experience, industry associations, and expertise in bringing these technologies to market, small community banks can develop an end to end disaster recovery and business resumption strategy that is effective and affordable.

Many of the security concerns surrounding the cloud has also been on the front burner for many of the large providers. To ensure the viability of incumbent torch bearers of the 90's technology boom, all eyes have turned to investing heavily in securing the cloud. Mainstays of the industry such as Microsoft has placed their highest priority in ensuring their technologies are the trusted conveyance by which companies will ride for the next 100 years. They understand that healthcare, governments, and financial institutions have heavy regulatory compliance burdens and if Microsoft can't meet them, their business will be overtaken by others who can.

The good news is the beneficiaries of all this investment is the market segment defined as the Small Medium Enterprises (SME). SMEs are characterized as having a disproportionate amount of technology burden per number of employees. A small community bank may have under 100 employees but have the technology requirements of much larger non-regulated companies.

Northstar Technologies is one technology partner that has fully embraced the cloud delivery model of applications and services and is ideally positioned to help community banks and SMEs with their cloud strategy. By partnering with the likes of Microsoft, Northstar can assist banks assess the value of embracing cloud services such as Office 365 and Azure public cloud offerings. Utilizing the ubiquity of cloud technology coupled with a high understanding of the security standards that need to be applied, Northstar has developed innovative disaster recovery offerings that are designed to weather even the most severe of geographic pandemic events. Designed specifically for regional banks who are deficient of hot or warm sites, Northstar is able to recover critical servers, data, workstations, and connectivity within minutes of declaration of disaster. Capped off with non-intrusive, annual disaster recovery testing services, Northstar provides an end to end DR solution that far exceed what was possible even a few years ago.

Northstar Technologies recently assisted RLR in moving to office 365 after a disastrous week where we lost our connectivity as a result of a Frontier Communications problem. Our transition to 365 was relatively seamless and rather fast thanks to Northstar Technologies. As many of our IT audit clients know, Northstar Technologies is our business partner for conducting internal and external vulnerability scans in conjunction with our IT audits.

Want to know more about Microsoft Security and Privacy? Check out these links:

- https://products.office.com/en-us/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy
- https://www.microsoft.com/en-us/trustcenter

NORTHSTAR TECHNOLOGIES

Ji Lee, Principal Analyst, Northstar Technologies

Ji.lee@nstnet.com : www.choosenorthstar.com

Consultant Spotlight

DINA MATIAS - RLR is pleased to introduce the newest member to our team, Dina Matias. Dina has over 25 years of experience in the financial industry. She has lead financial institutions in Operations, Risk Management, Electronic Banking and Compliance. Her most recent experience in the financial industry includes management of all aspects of Operations and Electronic Banking for a $4 billion southern California Bank, and management of the Electronic Banking Department and Call Center for a $20 billion southern California Bank. Dina is located in San Diego, California. Please join us in welcoming Dina to RLR. She can be reached at dina.matias@rlrmgmt.com

Upcoming Events

September 17-19, 2017	IBA Annual Conference	Des Moines, IA
September 17-19, 2017	AFT Fall Summit	Park City, UT

Did you know?

RLR delivers solutions through hands-on, personalized service. We offer our clients support and solutions to complex issues. We believe in partnering with our clients every step of the way to provide them with the evaluation, planning, design, and implementation of high quality, cost-effective solutions. Below are some of the projects RLR Management Consulting Inc. is currently working on. **How can RLR help you?**

- Operational Services
- Technology Services
- Regulatory Compliance
- Mergers & Acquisitions
- Due Diligence
- Staffing Services
- Audits and Related Services
- De Novo Services

RLR can also help with these HOT topics:

- Cybersecurity
- TRID – TILA-RESPA Integrated Disclosure
- NDIP – Non-Deposit Investment Products
- ADA Website Compliance

Contact Us

Reno, NV Office
6121 Lakeside Drive
Suite 135
Reno, NV 89503

Palm Desert, CA Office
77806 Flora Road
Suite D
Palm Desert, CA 92211
Office: 760-200-4800
Toll Free: 888-757-7330

- Ruth L. Razook ruth.razook@rlrmgmt.com
- Mitch Razook mitch.razook@rlrmgmt.com
- Tom Frale tom.frale@rlrmgmt.com
- Lynsey Bloch lynsey.bloch@rlrmgmt.com
- Jim Scott jim.scott@rlrmgmt.com

Find us on social media!

Visit our website www.rlrmgmt.com Send us an email info@rlrmgmt.com