Credit Union Directors NEWSLETTER

January 2022
Volume 48
Issue 1

Pandemic presents 'perfect storm' for fraud

Rise in unemployment claims and motivation to get money to those in need play a role.

The coronavirus pandemic has led fraudsters to take advantage of lax controls, overwhelmed organizations, and the desire to quickly get money into the hands of those who need it most, says Sue Landauer, certified public accountant and partner at Forensic Accounting Services Group LLC.

"We've had a lot of fraud, and we're still unraveling it all," says Landauer, who addressed the CUNA Supervisory Committee and Internal Audit Conference. "Fraud tends to increase when a crisis occurs. They tend to prey on us."

The most common types of fraud affecting credit unions during the pandemic involve unemployment benefits and Paycheck Protection Program (PPP) loans, she says.

Unemployment fraud

During the pandemic, the government issued $630 billion in unemployment benefits. But nearly 10% of that—$63 billion—were fraudulent claims, Landauer says. About $565 million has been recovered.

The Financial Crimes Enforcement Network (FinCEN) released an advisory Oct. 13, 2020, alerting financial institutions to fraud related to unemployment claims:

▶**Fictitious employer/employee fraud** involves the creation of a fictitious company with fake employees claiming to have been laid off during the pandemic. Criminals filed false unemployment claims.

▶**Employer/employee collusion** takes place while the employee receives unemployment benefits while still receiving wages—often under the table—at a reduced rate. The employer is aware and part of the fraud.

▶**Misrepresentation of income fraud** is when someone returns to work and fails to report the income or claims higher wages than what they were previously earning.

▶**Insider fraud** occurs when state employees use their credentials to access or change unemployment insurance claims. In these cases, fraudsters approve unqualified applicants or improper payment amounts, or deposit funds in accounts not on the application.

▶**Identity-related fraud** takes place when criminals use stolen or fake identification to file claims.

> "**FRAUD TENDS** to increase when a **CRISIS OCCURS.**"
>
> Sue LANDAUER

In a nonpandemic setting, unemployment claims would be verified with company human resources departments.

However, the pandemic made it difficult to do this because many employees worked from home, Landauer says. Added to that was the sheer volume of claims coming in, which overwhelmed unemployment agencies and added to the inability to verify claims.

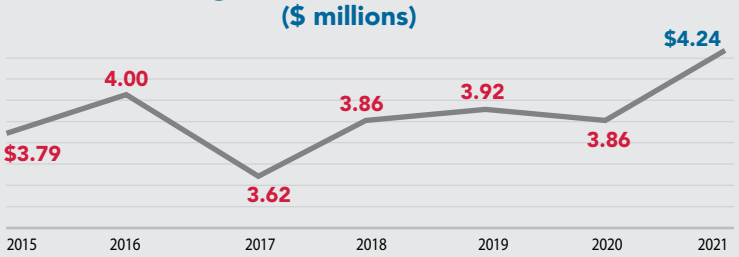
"The mandate was to get the money out to the people because they needed it," Landauer says. "It was the perfect storm for this type of fraud."

QUICK TAKE for your next board meeting

Rising data breach costs

The average cost of a data breach increased significantly in 2021, according to the IBM Cost of a Data Breach Report 2021. In 2021, the cost was $4.24 million, a 9.8% increase over the average total cost in 2020 ($3.86 million). The cost of data breaches has risen 11.9% since 2015.

Average cost of a data breach
($ millions)



Source: IBM Cost of a Data Breach Report 2021

PPP loan fraud

The CARES Act established PPP loans to assist businesses, but fraudsters found ways to take advantage of the program.

"We gave out these loans and, as long as they kept within [certain] parameters, the loans were forgiven by the government," Landauer says. "There was a lot of money to be taken. This was another classic example of getting money into the hands of businesses quickly."

Five examples of PPP loan fraud:

1. Falsely claiming the company has fewer than 500 employees.

2. Falsely claiming the coronavirus crisis hurt the business.

3. Inflating the average monthly payroll costs to get more loan money.

4. Falsely claiming all of the loan money was used for qualified expenses (payroll, rent, mortgage, utilities) to obtain loan forgiveness.

5. Not disclosing when employees left, thereby reducing payroll expenses, to get more of the loan forgiven.

The Department of Justice announced the first federal accusation of PPP loan fraud on May 5, 2020. Two men allegedly applied for a PPP loan for $543,882 and claimed they had "dozens of employees" earning wages at four different businesses. But the businesses had no employees and weren't operating prior to the start of pandemic, Landauer says.

As with unemployment fraud, Landauer says the pressure to process and disburse PPP loans quickly, the sheer number of applications, and failure to check payroll records played into the fraud.

"The world was at a standstill. The ways and means may have changed but the underlying frauds stayed the same," she says. "We have to make sure the opportunities for fraud don't exist and that controls are in place and functioning as designed."

Unemployment fraud: 6 red flags

Financial institutions need to monitor accounts for unemployment fraud, says Sue Landauer, certified public accountant and partner with Forensic Accounting Services Group LLC. She cites six red flags that could signal fraud is taking place:

1. Out-of-state unemployment insurance payments.

2. Multiple state unemployment insurance claims coming into the account.

3. Payments for different names than the accountholder.

4. Unemployment and direct deposits occurring simultaneously.

5. A high number of unemployment claims deposited into the same account.

6. Deposits that are quickly withdrawn or transferred.

"Hopefully someone in your credit union got this advisory and set up some system controls to look for these red flags," Landauer says.

Cannabis offers opportunities and risks

Have procedures in place to meet compliance requirements.

The cannabis industry's rise as a multibillion-dollar operation offers credit unions a promising new market, but one fraught with pitfalls.

Bruce Pearson, an attorney with the law firm of Styskal, Wiese, and Melchione LLP, says credit unions in states that have legalized marijuana generally fall into three groups: those that offer services to marijuana-related businesses (MRBs), those that refuse to do so, and institutions that have adopted a don't-ask, don't-tell stance regarding potentially disguised MRBs.

All face risks. Those providing banking services must meet strict compliance requirements.

But simply saying "no" to MRBs isn't enough.

"If you're going to be a 'no' shop, you need to have operational procedures to back that up," Pearson says. "Are you actively looking for MRBs that are disguised as car washes, window washers, and dry cleaners? If you're going to be a 'no' shop, are you driving off businesses that you can't get back someday?"

Credit unions that don't monitor loans that could be tied to disguised MRBs risk not only the seizure of collateral but could face prosecution under federal racketeering law.

"In court you literally have to prove a negative: I didn't know and I had no reason to know that the collateral was being used in a criminal enterprise," Pearson says. "If you're seeing the deck stacked against you, you're right."

Pearson's advice for the don't-ask, don't-tell crowd is simple: get into one of the other two categories.

Credit Union National Association
CUNA

CUNA GAC is back in D.C.

Join thousands of your peers to show lawmakers what the #CUDifference is all about.

Register at cuna.org/gac2022

2022 CUNA GAC

FEB 27 — MAR 03 CUNA GOVERNMENTAL AFFAIRS CONFERENCE

Credit Union National Association
CUNA

AVAILABLE THROUGH
SEPTEMBER 11, 2022

Adapt strategic plans with insights from current industry trends

CUNA

Trends into Action

eSchool (RECORDED)

At CUNA Trends into Action eSchool (recorded), credit union leaders and board members will learn about four key industry trends important for consideration as they engage in strategic planning.

The content and trends covered, compiled from the 2021-2022 CUNA Environmental Scan, address the current industry environment. Board members will receive expert analysis of how current trends may evolve and ways to plan for those possibilities.

cuna.org/trendseschool

Preparing for cyberattacks

Develop an incident response plan to limit exposure time during cyberevents.

The global average amount of time to identify and contain a data breach is 280 days: 207 days to identify the breach and another 73 days to contain the attack, according to IBM's "Cost of a Data Breach Report 2021."

Financial institutions fare better, with a 233-day average response time (177 days to identify a breach and an additional 56 days to contain the attack). But that's still plenty of time for hackers to steal information.

"The bad guys can do a lot in 177 days," says Randy Romes, principal at CliftonLarsonAllen LLP. "They're inside learning your business."

Romes discussed cybersecurity threats and how credit unions can prepare and respond during the CUNA Supervisory Committee and Internal Audit Conference.

According to the IBM report, the average cost of a data breach in the U.S. is $4.24 million. Eighty percent of breaches include records containing personally identifiable information at an average cost of $150 per record.

Hackers can do a lot in the time it takes organizations to discover and contain an attack, Romes says, such as disabling backups and security systems, obtaining access credentials, stealing sensitive personal data, and creating back doors for entry into the system.

Ransomware gets the most attention, but Romes says it's usually coupled with other acts and is simply the most visible part of an attack.

The first step after a ransomware attack is resuming operations, he adds, but there are also legal and business ramifications that will persist after the breach.

"Ransomware is what they do as they're walking out the door," he says. "They've already been in, taken over accounts, and taken our data."

Eighty percent of breaches have a root cause in email spear phishing or other social engineering efforts where hackers enter systems when employees click on phishing links in emails or harvest data by guessing passwords.

"Be prepared," Romes says. "This is going to happen. How do we turn the 177 days into seven days? You must shorten the time frame to limit your exposure."

Organizations must develop an incident response program and plan that includes response procedures and a list of appropriate contacts. To prepare, determine who will handle certain tasks, collect their contact information, determine how they'll operate once an attack has occurred, and what the cost will be, he says.

After developing the plan, practice it. Carry out tabletop exercises to walk through incident and response procedures, spear phishing tests, other social engineering tests, and "Red Team" penetration testing, which is more targeted than traditional penetration testing, Romes says.

One thing is certain. Cyberattacks will happen, Romes says.

"Not if. When. What are you going to do about it? You must prepare, implement, and practice a plan."

Data breach resolution

$4.24 million
Average cost of a data breach

177
Days to identify a breach

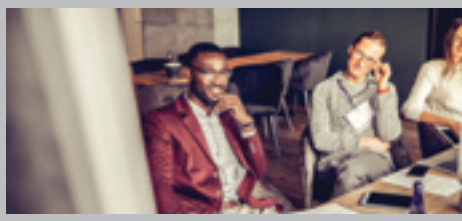
56
Days to contain the attack

Source: IBM Cost of a Data Breach Report 2021

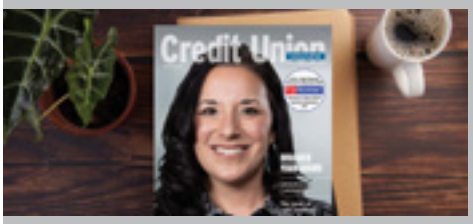
Resources

CUNA Governmental Affairs Conference, Washington, D.C., Feb. 27-March 3: *cuna.org/gac*

CUNA board and committee solutions: *cuna.org/board*



CUNA Board of Directors Community:
community.cuna.org



Credit Union Magazine:
news.cuna.org/creditunionmagazine

Beware the 'Green Rhino'

Is climate change part of your risk strategy?

Business strategist Michele Wucker developed the notion of the "Gray Rhino"—a highly probable, high-impact, yet neglected threat.

Such threats are not random surprises but occur after a series of warnings and visible evidence. In today's risk environment, that rhino is climate change.

Tony Ferris, CEO of Rochdale Paragon Group, refers to climate risk as the "Green Rhino," with the green representing the environment.

"It's camouflaged; we can't see the direct correlation to our businesses today," he says. "We tend to discount that so it gets pushed off due to a lack of understanding of what the implications might be on business today."

Some argue the most obvious impacts of climate change are increased wildfires in the Western U.S. and a more volatile hurricane season in the Southeast. While those natural disasters result in lost property and loan defaults for credit unions, Ferris views them as business continuity events more than strategic risks.

As a longer-term example, he cites the recent announcement that all passenger vehicles in California will be zero emission by 2035.

"Auto lending is one of credit unions' biggest asset plays," Ferris says. "If you're moving to all electric and hydrogen vehicles, what does your new business model look like? Is it good for you? Is it bad? What happens to the used cars in that market?"

Other regulatory changes are in the works, says Ferris, citing the Biden administration's climate and environment priorities.

Such changes influence how credit union members conduct their day-to-day financial affairs, he notes. "Big climate-related changes directly affect how consumers pay for energy. That has a trickle-down effect on consumer spending."

One way credit unions have addressed this challenge is by offering solar loans.

"Risk is another term for opportunity," Ferris says. "It's two sides of a coin. It's about understanding where those opportunities exist within your membership and organization."

Regulators have issued little guidance on climate change, although Linda Lacewell, superintendent of the New York State Department of Financial Services, issued a guidance letter in October 2020.

Also, in November the Federal Reserve issued a statement supporting global efforts to identify key issues and potential solutions for climate-related challenges.

Ferris expects more regulatory guidance within the next year. As for now, he says credit unions should consider climate risk from an outward rather than internal risk perspective.

"Keep an eye on trends you see in the news," Ferris says. "Self-driving cars are a great example. A few years ago they weren't nearly as viable as they are today."

He advises credit unions to use that information when developing their risk strategy.

"The letter from the New York regulator recommended putting climate change in your risk management program and developing a focus on it," Ferris says. "Have the discussions, be cognizant of it, and brainstorm so it doesn't catch you off guard and you continue to evolve your thinking."

> **"Risk is another term for opportunity."**
>
> **Tony Ferris**

CREDIT UNION DIRECTORS NEWSLETTER
(ISSN 1058-1561) is published monthly for $157.50 per year by the Credit Union National Association, 5710 Mineral Point Road, Madison, WI 53705-4454. (Multiple-copy discounts available.) Also available as a downloadable PDF for an annual subscription rate of $773. Periodical postage paid at Madison, Wis.

POSTMASTER
Send address changes to CREDIT UNION DIRECTORS NEWSLETTER, P.O. Box 431, Madison, WI 53701-0431. Advertising is accepted only from reputable firms, but inclusion of advertising does not imply endorsement by the newsletter or CUNA Inc.

EDITORIAL STAFF
MICHELLE WILLITS // publisher, mwillits@cuna.coop
BILL MERRICK // deputy editor, bmerrick@cuna.coop
JENNIFER PLAGER // managing editor, jplager@cuna.coop

DESIGN AND PRODUCTION STAFF
CARRIE DOYLE // graphic designer, cdoyle@cuna.coop

CONTACT INFORMATION
EDITORIAL // 608-231-4290
SUBSCRIPTIONS // 800-356-9655, or cuna.org/directors