

# Branch of the future

## Risk overview



There are many opinions why an organization should move to the branch of the future... including efficiency, convenience, flexibility, stronger relationship engagement, and even better reflecting your members. No matter the reasons, the decision is often fueled by combining technology, creative design, and high-touch service.

While many consumers love digital channels for transactional activities like deposits, transfers, and payments – most still want human touch for lengthier topics, complex issues and more-involved discussions.

Today's consumer evaluates financial institutions based on their user experience. Much like online shopping, or making a dinner reservation on their mobile device, consumers expect their banking experience to be seamless and instantaneous.

This strategic discussion and branch transformation is critical and one in which you must balance an engaging member experience with sound operations and emerging risks in mind.

Each reimagined branch has a much different risk and threat profile to be considered.

### **Myth: digital channels are killing branches**

- Consumers love digital channels for transactional activities like deposits, transfers, and payments
- Most still want human touch for lengthier topics, complex issues and involved discussions
- Investments in technology and staffing must reinforce the credit union's strategy
- Well-placed branches can serve as critical foundations in the communities you serve

## What does the branch of the future look like?

It depends and it isn't a one-size-fits-all.

- Micro-branches with reduced staff.
- Open concept with concierge-type service.
- Operate within mobile branches, grocery or other retail locations.
- Provide new ways to interact with staff in priority areas, through extended hours, or even from employees working at other locations or from home.
- Be "phygital" by blending physical and digital experiences.
- Incorporate a café or other multi-use facilities such as children's access, community rooms, onsite daycare, and/or fitness facilities.
- Be established with a range of smart technology like cash recyclers, interactive teller machines, smart boards, and even robot greeters.
- Simply be extended hours, an off-site ATM, or online appointment scheduling.

## Branch of the future changes drive new risks to consider

### Next generation vulnerabilities

Enhancing customer experience through innovative technological products and solutions can put your credit union at a competitive advantage; however, these changes can also introduce new and different risks.

- These technological advancements can require risk oversight related to:
- Member education on technology use and helping them protect their own data.
- Technology support – such as automatically clearing browsing history & cookies.
- Member authentication – knowing and validating your members.
- Adaptability & compliance with ever-changing rules and regulations such as ADA (Americans with Disabilities Act); UDAAP (Unfair, Deceptive, and Abusive Act Practice); and CCPA (California Consumer Protection Act).

### Safety & security

Highly-automated micro-branches focused on member interaction or even a kiosk location with individual ATMs or remote tellers brings a much different threat profile than your traditional, full-service branch location. It can present a different risk of harm or some type of threat looking to take cash from either your member or from your employees.

A big component is developing a plan around safety, security, and response for each of your individual locations.

You'll need to consider physical security issues like robbery, burglary, and active shooter incidents; cybersecurity and system access; branch access for staff, members or the community; disaster recovery and business resumption activities; and ensuring your internal control policies and procedures still align.

### Employee roles & skills

While a branch redesign and integrating technology is important, don't forget about your employees.

A reimagined branch can have impact on your employees and risks associated with changes in their roles and functionality, such as:

- Being comfortable in a sales and consultative engagement – possibly based on analytics - rather than transactional-driven activities
- Adaptability with technology and new settings – especially, as it can relate to talent management of multi-generational staff
- Concerns involving human resources and workplace set-up within the office or remote work arrangements.
- Reduced or realigned staffing with the smart branch concept transforming your member interaction needs

## Transformation through technology

The adoption of digital technology has led to more efficient delivery channels and with this innovation credit unions can typically deliver products and services more quickly and at a lower cost.

Traditional branch models have typically relied on a siloed approach to channel management separating mobile, online, and branch locations. This has created neither a member friendly nor efficient staff experience as each channel requires its own set off workflows, governing documents, content creation, and risks.

### Customer-centric digital structure more viable?

While many credit unions are implementing a wide range of tech solutions, some are focused on digital banking platforms consisting of several interrelated components, such as:

**Omni-channel banking** typically streamlines all channels and enhances the member experiences at any touchpoint. A winning omni-channel platform begins with a clear member journey – whether it be digital or human.

**Smart banking** technologies and tools such as artificial intelligence and data mining are also increasingly used to create hyper-personalized services and communications. Automated behavioral tracking solutions provide insights into member needs, enabling credit unions to offer more personalized advice and offers quickly.

For example, a consumer browsing real estate products could be presented with an appropriate mortgage offering. This method of tracking consistently caters to personalized needs while positioning the credit union as a trusted partner with their member's best interests in mind and makes for a more meaningful experience.

**Identity and access management** is key to ensuring access security in a digital banking environment. A sophisticated entitlements solution makes this easy, by automating and managing the process of granting access rights to trusted users.



Smart branches employ a wide range of technology solutions. Here are some of the most popular technologies based on the percentage of FIs implementing:

- Digital signage
- Interactive kiosks
- Tablet kiosks
- Interactive teller machines
- Overhead music
- Video walls
- Video conferencing

Even though some of these new tech changes have a small footprint, they tend to introduce convenience and high-touch accessibility into the reimagined branch.

## Additional risks to consider

Regardless of whether decisions are made by an employee or an algorithm, on a mobile app or inside a branch, a critical component of all credit union business functions is the need to mitigate against risk.

### Execution risks

A credit union's digital aspirations may hinge on reducing reliance on legacy systems as well as de-cluttering and decommissioning redundant solutions. Launching an entirely new digital entity alongside existing legacy organization may also be necessary. Both these options create risks related to cost, talent management, redundant workflows, and governance failures.

### Supply chain governance

Whenever implementing new technologies, enhanced governance structures and risk frameworks are necessary to ensure safe integration. This includes identifying certain threat vectors arising from threats such as software supply chain vulnerabilities.

### Accessibly risks

Credit unions should strive for all electronic and information technology to be accessible to all who wish to access them. Color, font size, and clickable links should be designed with all consumers in mind, including those with certain disabilities.

### Vendor reliance risks

Once a digital delivery model is firmly in place, many institutions may find they heavily rely on vendors for execution and resources. Over time, some come to be so reliant on vendors / contractor for critical knowledge on certain solutions that they have, in fact, ceded control to the vendors. This poses risks such as loss of an ability to control ongoing costs associated with those solutions, poor data governance, and weak succession plans.

### Keyperson risks

A keyperson is an employee with proven skill and tactical knowledge in a business area. They have delivered individually superior performance within their department, know exactly where to find useful information, and know which are the best methods and tools in any circumstances. If exposed to these sorts of risks in digital delivery models a credit union could face decreased productivity, profitability or reputation simply by the departure of one or a few keypersons.

### Strategy consideration: investing in digital technology

- Develop a member experience, data-driven, digital journey that begins when a customer contemplates buying an asset, not when he/she comes looking for a loan to finance that asset.
- Workforce and culture practices should adapt to attract and retain multi-generational talent. Rigorously cross train staff and welcome talent from outside of traditional financial institutions to become more diverse and welcome new solutions and opportunities to optimize digital transformations.
- Increasing sophistication of cyber-attacks is placing a new premium on protection of existing value. Advance governance models, risk frameworks, talent management and automation should be used to mitigate risks.
- A widespread cultural change must precede technology upgrades and investments. Culture is what aligns an organization's effort to do things well, or to do things poorly. Understanding your credit union's digital culture is composed of the collective experiences of employees - what they believe in and what they value.



## The cloak of anonymity

The online channel has quickly become a valuable tool in providing member convenience – like account opening, loan applications, and other banking transactions. However, fraudsters also enjoy more obscurity challenging credit unions in properly authenticating and verifying members and potential members.

Member authentication was easier years ago, when your members and potential members walked through the credit union doors. Data breaches have fueled the problem since they often lead to identity theft.

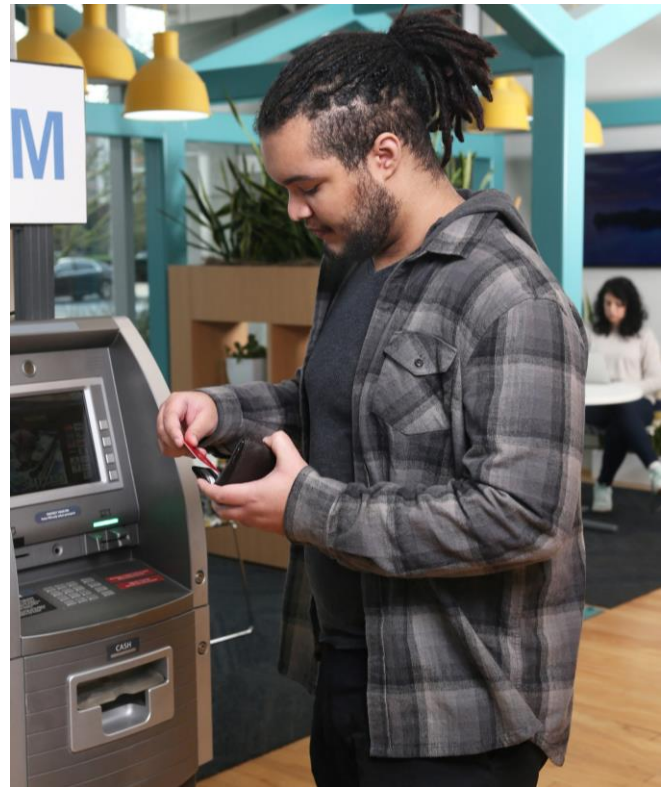
The uptick in Social Security Number compromises, in addition to other easily accessible, personally identifiable information (PII) – names, addresses, and birth dates - from these breaches compounds the problem with the introduction of synthetic identity theft. The stolen personal information has significantly increased the number of identity theft-related fraud losses reported.

### Common fraud losses involving authentication

- New Account Fraud
- Loan Fraud
- Call Center Fraud and member impersonation
- Account Takeovers

Fraudsters also continue to visit branch offices, making it critical for staff to be alert and cautious when opening accounts and processing loan applications.

The Fair and Accurate Credit Transactions Act (FACT Act) requires credit unions to adopt a written Identity Theft Prevention Program to detect, prevent and mitigate identity theft in connection with the opening of a covered account or existing covered accounts. Ensure your program is up-to-date to reflect today's identity theft fraud environment and staff in key positions are adequately trained.



The credit union branch as we know it, with tellers behind windows and new account or loan MSR's (Member Service Representatives) huddled in cubicles with desktop computers is being reinvented at rapid pace. In fact, these smart branches use technology to boost sales and improve customer experience significantly with little distinction of the staff.

For example, tablets give MSR's the freedom to roam the branch — much in the way that Apple Store employees do — enabling them to increase sales and provide superior customer service. In addition, teller cash recyclers (TCR)/ teller cash dispensers (TCD), interactive teller machines (ITM), kiosks, tablets and video monitors provide self-service access to transactions and money.

## Workplace & employee safety

---

The inherent advantages of open concept branches, micro-branches, and other branch of the future approaches can also have their potential drawbacks, some of which relate to security.

For example, easy access to terminals and kiosks can effectively handle money more efficiently than tellers – but it also gives thieves and hackers the opportunity to manipulate machinery, claim to be someone that they're not, or coordinate an incident. In addition, potential frustrated disturbances – such as a member distraught over a lost credit card or being a victim of a scam - requiring prompt and proper staff escalation.

If you take security lightly, your credit union, employees, and your members could soon encounter widespread problems.

### Considerations for non-traditional branches

- Be aware surroundings and looking for unfamiliar faces, especially at nontraditional branches located in higher activity areas.
- Branch employees located within a building open 24/7, such as hospitals, should remain more alert. If opening/closing during employer staff transition times, be cautious of your surroundings. Watch for individuals that are focused specifically on your movements and actions.
- Determine an all-clear signal for one-person branches. Consider an email or text to another employee.
- Don't present yourself as a target by leaving the branch prior to opening hours. While it may be tempting to go next door to quickly grab a coffee, this routine can be easily spotted by a potential robber.
- If your credit union has an ATM foyer that has to be entered or exited as part of the opening or closing procedures, staff should wait until it is empty prior to initiating either procedure.

### Curbside service

Credit union curbside service is often offered by appointment for member services such as account/loan document signing, pick-up/drop-off, notary services, certificate renewals, and replacement debit cards. With any operational change, it is critical to have a plan for ensuring a safe environment in each type of location and service. For curbside service, employee safety should be considered – especially with an increased risk of slip, trips & falls with winter-like weather entering the picture

- Review credit union location security procedures to identify any employee safety issues. Follow well-thought-out procedures to help make your credit union a less attractive target for unwanted situations.
- Ensure the curbside area, walkway, parking lots and all sides of the credit union building have outside cameras that are operational and positioned to capture footage. Periodically test video surveillance and lighting to verify it is in proper working order.
- Identify/control safety hazards - Use a hazard analysis process that focuses on the tasks that employees complete, describes tasks, and assesses the inherent hazards to those tasks.
- Maintain written safety programs - Outline the expectations of employees when it comes to safety in the workplace, as well as how you will meet regulatory requirements.
- Create good housekeeping practices. Avoid creating obstacles in entranceways, aisles, stairwells, and walkways
- Reduce wet or slippery surfaces on parking lots; sidewalks; floors in general. When possible, salt and other de-icing agents should be applied immediately prior to snow and ice storms to minimize freezing.
- Offer periodic safety tips and encourage employees to share tips of their own.
- Any time an incident occurs in the workplace, the employee injury should be reported immediately.

## After-hour & community spaces

Members, community groups, and non-profit organizations often look to local business facilities to host their meetings and events. Credit unions often fit the bill. Some credit unions allow employee access to the exercise facility during nonbusiness hours. In some cases, guests of employees have also been allowed in after hours.

In fact, many credit unions have allowed access to meeting rooms or have even built new facilities with the intention of adding community rooms specifically. In addition, onsite workout and exercise facilities are being added to retain and attract talented staff.

However, those benefits can be overshadowed by injury risk and potential liability issues, security concerns, and property damages, if proper mitigation steps are not implemented.

In addition to granting authorized access to staff, your credit union may need a secure way to permit temporary access to a certain area for a short period of time. If you receive unattended deliveries or need to schedule unsupervised repairs or other visits, a visitor management solution can help.



- Implement a facilities use/access policy that creates a clear understanding between the credit union and the users of the facilities. At a minimum, address the hours of use, limit the use to employees, promote the buddy system, and address the maintenance of equipment.
- Complete periodic inspections of the facilities and outside areas to identify potential hazards that may cause slip, trip, falls, or other safety issues. Do not allow smoking, alcohol, cooking, open flames, or unlawful activities.
- Review security issues. Having a credit union employee present to open and close the facilities is a best practice. Maintain strict access to credit union keys and / or alarm code. The credit union office should not be accessible by anyone using the facilities and should be on its own alarm zone allowing the credit union office and safe / vaults alarms to be active.
- Require users to sign a legally-approved waiver of liability indemnifying the credit union, as well as providing a medical release stating they are physically able to use the facility. The waiver should clearly state that use of the facility is not part of the employee job description to minimize risks of potential workers compensation claims.
- Have all policies and agreements, including the waiver of liability and medical release, reviewed and approved by the credit union's legal counsel for compliance with laws and regulations.

## Risk controls to implement

### Open branches & concierge service

- Mount visible transaction cameras on workstation and throughout the credit union
- Reduce currency at teller desks
- Position workstation/pods so they can be observed by many
- Restrict how much currency the TCD/TCR can disperse per transaction
- Consider have a greeter to direct member traffic, this may also be a deterrent to robbers
- Position pods as far away from entrance/exit door as possible
- Work with reputable vendor to achieve the correct balance between employee's safety and the desired member experience
- Position pods so they be observed by multiple employees

### Teller cash recyclers/dispensers

- Consider putting a limitation on teller or transaction, before an override is needed
- Implement forced dual control on currency and reduced amount per transaction
- Implement a robbery code
- Ensure currency is in a secured chest
- Have teller drawer at station

### Interactive / Personal Teller Machines

- Address in training how to respond if a robber goes to a machine and asks the remote teller for money
- Make sure the area or room is private
- Have a chest designed for 24-hour use
- Forced dual control to access chest
- Member identification safeguards

### Children's areas

- Are there any toys or equipment swallowing or choking hazards?
- Does equipment or office furniture have unprotected edges?
- Is there sufficient camera coverage of the area?
- Are cabinets, bureaus, and shelving attached to the wall?
- Is the children area inspected for hazards throughout the day?

### Exercise facilities

- Have a facilities usage policy so staff is aware of what is and is not allowed
- The policy should be designed with the intent of the safety and security of both the employee and the credit union
- Require users to sign a legally-approved waiver of liability indemnifying the credit union, as well as providing a medical release stating they are physically able to use the facility
- Don't allow improper use and maintenance of exercise machines and free weights
- Don't allow portable workout items such as exercise balls and small free weights at desks and break rooms
- Hire only certified trainers / instructors to lead exercise programs at the office

Understand how employees working in a different state than which the credit union is located can be impacted.

The laws and regulations effecting remote employees of the state in which the employee has set up their remote office must be followed as opposed to the laws and regulations of the state where the credit union is located.



## Success hinges on newly-skilled and engaged employees

Look to the people who already work at your credit union, regardless of their current role, to identify what needs to be done regarding training, policies, and procedures – especially with the advent of the new branch layouts and technology.

Each branch location presents a different risk or some type of threat. A significant component is empowering your branch managers and their cross-functional teams to develop an idea and plan for their individual locations. They're the ones working there, understand the operational details, and are most familiar with the location.

Training is key as service representatives no longer just handle simple transactions. Instead, members or potential members are often approached by employees who guide them to intuitive pieces of technology or assist them directly on their tablets.

Encourage your staff to focus on building relationships; establishing comfortable connections; and delivering their messages through a consultative approach.

Remember, almost all branch employees will need to be multitasked at sales and service and know how to use technology and devices for education and transactional purposes.

Consider these strategies to best prepare:

- Retool employees' skills and embrace the human touch equipping staff for digitally-infused service and sales to help members.
- Invest in branch talent and consultative training to assist with complex questions and decisions on all products / services.

## Employee development

- Create opportunities for mentoring – generating the opportunity to learn from each other.
- Ensure everyone understands the credit union philosophy and how your credit union fits into your community
- Identify different work styles and habits
- Understand preferred methods of communication, terminology, ideology, and the technology learning curve
- Consider extended hours – possibly requiring assistance from 5-8 pm, early mornings, or even Saturday afternoons
- Consider branches, job responsibilities, or ergonomic needs that involve open office concepts, standing for long periods of time
- Have a well-defined employee handbook (reviewed by legal counsel) that addresses flexible workplace policies, work hours, dress codes, etc.
- Consider a diverse set of employee benefits such as daycare services; quiet or recharge rooms to relieve stress; meditation, office massage, yoga or workout classes; onsite fitness facilities or discounts; game rooms; lactation rooms; eldercare services for those caring for parents; ergonomic and innovative workspaces; and student loan repayment or tuition reimbursement options
- Ensure employment laws and regulations are being followed to protect both the credit union and your employees
- Check assumptions and biases. Recognize behavior and how it affects others. Support collaboration, borderless teams, and flexible work arrangements

Clearly, branches continue to be important, but that doesn't mean they can maintain the status quo. Many suggest that branches remain the dominant channel for account opening, highly interactive transactions, and financial consultation. However, the transformation isn't simple.

As competitive businesses, you need to ensure the financial reward or upside is compelling enough to invest in the branch of the future, new technologies, and partnerships.

Infrastructure can greatly influence the success or failure, particularly those that are disruptive, innovative, or highly technical in nature. Infrastructure is not only important during research and strategy development, but also once your solution, product or service is ready to be implemented hit the market, it must have the right infrastructure to support it.

It is critical for you to connect strategy to risk management. To strike the right balance between physical and digital footprints and the connected risks, consider these strategies:

- **Research what matters**...know your market. Member types; transaction mix; demographics; demand; preferred customer journey
- **Blend the human touch with technology** including staffing and service models.
- **Invest in the branch** - Staff talent & realignment; budget implications; technology adaptability; branch interaction; and workforce ability to change
- **Execute strategies with risks in mind.**

## Looking for additional insights?



- Access the **Business Protection Resource Center** (User ID & Password required) for exclusive risk and compliance resources to assist with your loss control efforts.
- Go to **Emerging Risks Outlook** for critical questions, answers, and resources to help build additional awareness and drive organizational action.
- If you'd like to discuss this risk in more detail, simply schedule a no-cost 1:1 discussion with a TruStage™ Risk Consultant by contacting us at [riskconsultant@trustage.com](mailto:riskconsultant@trustage.com) or at **800.637.2676**.

This resource is for informational purposes only. It does not constitute legal advice. Please consult your legal advisors regarding this or any other legal issues relating to your credit union. TruStage™ is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions, and exclusions.