BREA Meeting Minutes
July 14, 2026 at 1:00 pm
Via Zoom

Minutes recorded by Mona Rowe
Contact Information:
Brookhaven Retired Employees Association BREA
BNL Bldg. 400A
BERA Recreation/ Attention BREA Meeting
Upton, NY 11973

Present: Les Fishbone, Louise Hanson, Mark Israel, James Lemley, Arnie Moodenbaugh, Steve Musolino, Mona Rowe, Steve Shapiro, Barry Siskind, Ed Sperry, Charles Weilbrenner, Gwyn Williams
Guests: Mr Ho Yin Leung (VP of Fraud at Teachers Federal Credit Union) and Chitresh Sen (Cyber and Risk Leader at Teachers Federal Credit Union)

Officers 2024-2026: President: Arnold Moodenbaugh, Vice President: Due to the sudden passing of Andy Feldman, this is now an open position; Secretary: Laura Miller, Treasurer: Louise Hanson

TFCU presentation on fraud

Before the BREA meeting, two representatives from Teachers Federal Credit Union, Ho Yin Leung (VP of Fraud) and Chitresh Sen (Cyber and Risk Leader), talked about fraud, which is a fast-growing threat in the United States.

The presenters gave some simple advice, some of which came in answers to questions from retirees:

- If you do not recognize a call on your phone, don't take it. If you decide to take the call, say nothing first.
- When you respond to a call, the bad actor is harvesting your voice to create a digital representation of it.
- Look up Regulation E, which is a federal rule enforcing the Electronic Fund Transfer Act. It protects consumers engaging in electronic fund transfers by limiting your liability for unauthorized transfers.
- Nine out of ten cyberattacks start with phishing, with the intent to harvest your user ID and password.
- It's safer to make payments through credit cards.
- When something happens, freeze your account.

The presentations can be found in Appendix A of these minutes.

BREA Business

Because the TFCU presentation took close to an hour, Mona was unsure of when we started the BREA business meeting, but it was a few minutes past the hour.

Treasurer's Report: Louise read her report to those in attendance. A motion was made to approve the report, which was approved.

Membership Report: Betty sent her report ahead of the meeting and it was provided by Arnie. At the time of this meeting, we have 207 members, 191 members with email, 451 in 'arrears'. The Membership Report was then approved.

Betty included a summary of her efforts to resolve the membership list she received from HR. Melissa Schumann had sent her a list of deceased retirees. Betty combed through it and found five employees on the list who were also BREA members. She is to be applauded for her efforts to make sense of the way the information was entered into the database.

The CAC is on hiatus until the September meeting.

Tesla Center: Update from Steve Shapiro. They are still trying to stabilize the building, but they did open a visitor center, separate from Tesla's laboratory.

Arnie will write a letter of thanks to the Teachers Federal Credit Union speakers.

The meeting was adjourned at approximately 2:36 p.m.

The next meeting will be September 8th at 1:00 pm via Zoom.

Appendix A: Fraud and Cybersecurity Industry Trends

Cyber Threats on the Rise

How **attackers** are targeting financial institutions and their members —and the trend behind each.

1 Phishing & Social Engineering

HOW IT HAPPENS

- Fake emails and texts mimic trusted brands
- Links harvest logins and passwords
- AI makes the lures nearly flawless

INDUSTRY FACT
Voice and SMS phishing draw 40% higher click rates than email (Verizon 2026 DBIR).

2 Ransomware & Malware

HOW IT HAPPENS

- Malware locks systems and data for ransom
- Spreads via attachments and fake downloads
- Financial services are a prime target

INDUSTRY FACT
Cybercrime losses hit a record $20.9B in 2025, ransomware among the costliest (FBI IC3).

3 Data & Credential Theft

HOW IT HAPPENS

- Breaches expose members' personal data
- Reused passwords unlock more accounts
- Third-party vendors widen the attack surface

INDUSTRY FACT
Exposed-credential volume surged 160% in 2025, fueling account attacks (industry reports).

4 Third Party Risk

HOW IT HAPPENS

- Employees at a third-party vendor were tricked
- Attackers gained access through human error, not system failure
- Data was stolen and used for extortion

INDUSTRY FACT
Third-party security incidents now account for 30% of all data breaches worldwide (Industry reports)

Protect Yourself & Your Accounts

A few simple habits **stop** most of the fraud and cyber attacks before they start.

1 Secure Accounts and Devices Up To Date

WHAT TO DO

- Turn on Multi Factor Authentication (MFA) everywhere
- Use long, unique passwords
- Keep devices updated

WHY IT MATTERS
MFA blocks nearly all automated account-takeover attacks (CISA).

2 Verify Before You Trust

WHAT TO DO

- Never share codes or PINs
- Call the number on your card
- Avoid unexpected links
- Be skeptical of unexpected emails

WHY IT MATTERS
A quick pause to verify defeats most AI-driven scams (FBI).

3 Monitor & Report Fast

WHAT TO DO

- Set transaction alerts
- Review statements and credit reports
- Report fraud fast
- Recognize and report suspicious communications

WHY IT MATTERS
Early detection sharply limits fraud loss (FBI IC3).

4 Guard Your Identity

WHAT TO DO

- Freeze your credit at all three bureaus
- Watch your credit report for accounts you didn't open
- Limit sharing your SSN and personal details

WHY IT MATTERS
A credit freeze stops criminals from opening new accounts with a stolen or synthetic identity (CFPB).

Questions?

Sources

Federal Trade Commission (FTC)
Consumer fraud losses and imposter- and payment-scam reporting, 2025.
ftc.gov

Federal Reserve (Boston Fed)
Synthetic identity fraud loss estimates and generative-AI trend analysis, 2025.
federalreserve.gov

FBI Internet Crime Complaint Center (IC3)
Account-takeover and cybercrime loss figures, plus fraud-reporting guidance, 2025.
ic3.gov

Consumer Financial Protection Bureau (CFPB)
Credit-freeze and identity-theft protection guidance for consumers.
consumerfinance.gov

Verizon Data Breach Investigations Report (2026 DBIR)
Phishing and social-engineering click-rate data.
verizon.com/dbir

Cybersecurity & Infrastructure Security Agency (CISA)
Multi-factor authentication effectiveness guidance.
cisa.gov

Industry credential-exposure reports (2025)
Exposed-credential volume and related account-attack trends.

Sources

Federal Trade Commission (FTC)
Consumer fraud losses and imposter- and payment-scam reporting, 2025.
ftc.gov

FBI Internet Crime Complaint Center (IC3)
Account-takeover and cybercrime loss figures, plus fraud-reporting guidance, 2025.
ic3.gov

Verizon Data Breach Investigations Report (2026 DBIR)
Phishing and social-engineering click-rate data.
verizon.com/dbir

Cybersecurity & Infrastructure Security Agency (CISA)
Multi-factor authentication effectiveness guidance.
cisa.gov

Industry credential -exposure reports (2025)
Exposed-credential volume and related account-attack trends.

Federal Reserve (Boston Fed)
Synthetic identity fraud loss estimates and generative-AI trend analysis, 2025.
federalreserve.gov

Consumer Financial Protection Bureau (CFPB)
Credit-freeze and identity-theft protection guidance for consumers.
consumerfinance.gov

Fraud Threats on the Rise

How scammers are targeting members across the industry —and how fast each threat is growing.

01

Imposter & AI Voice Scams

HOW IT HAPPENS

- Callers pose as your bank, a vendor, or the government
- Urgent demand for a code, gift card, or transfer
- AI voice clones now mimic people you know

INDUSTRY FACT

Imposter scams were 2025's mostreported fraud— $3.5B lost, nearly 3x since 2020 (FTC).

02

Account Takeover

HOW IT HAPPENS

- Stolen passwords from breaches and phishing
- SIM swaps intercept one-time passcodes
- Contact info changed, then funds drained

INDUSTRY FACT

$262M in reported accounttakeover losses in 2025 (FBI IC3).

Fraud Threats on the Rise

How scammers are targeting members across the industry —and how fast each threat is growing.

03

Payment & P2P Scams

HOW IT HAPPENS

- Rushed Zelle, wire, or P2P to a new payee
- Romance, prize, or investment lures
- Check washing and mobile-deposit scams

INDUSTRY FACT

Consumers reported a record $15.9B in fraud losses in 2025, led by payment scams (FTC).

04

Synthetic Identity Fraud

HOW IT HAPPENS

- Real and stolen details are stitched into a brand-new identity
- Fraudsters build credit for months, then “bust out” and vanish
- Generative AI mass-produces convincing fake IDs and faces

INDUSTRY FACT

Synthetic identity fraud losses topped $35B, accelerated by generative AI (Federal Reserve, 2025).

Cyber Threats on the Rise

How attackers are targeting financial institutions and their members —and the trend behind each.

01

Phishing & Social Engineering

HOW IT HAPPENS

- Fake emails and texts mimic trusted brands
- Links harvest logins and passwords
- AI makes the lures nearly flawless

INDUSTRY FACT

Voice and SMS phishing draw 40% higher click rates than email (Verizon 2026 DBIR).

02

Ransomware & Malware

HOW IT HAPPENS

- Malware locks systems and data for ransom
- Spreads via attachments and fake downloads
- Financial services are a prime target

INDUSTRY FACT

Cybercrime losses hit a record $20.9B in 2025, ransomware among the costliest (FBI IC3).

Cyber Threats on the Rise

How attackers are targeting financial institutions and their members —and the trend behind each.

03

Data & Credential Theft

HOW IT HAPPENS

- Breaches expose members' personal data
- Reused passwords unlock more accounts
- Third-party vendors widen the attack surface

INDUSTRY FACT

Exposed-credential volume surged 160% in 2025, fueling account attacks (industry reports).

04

Third Party Risk

HOW IT HAPPENS

- Employees at a third-party vendor were tricked
- Attackers gained access through human error, not system failure
- Data was stolen and used for extortion

INDUSTRY FACT

Third-party security incidents now account for 30% of all data breaches worldwide (Industry reports)

Protect Yourself & Your Accounts

A few simple habits stop most of the fraud and cyber attacks before they start.

01

Secure Accounts and Keep Device up to date

WHAT TO DO

- Turn on Multi Factor Authentication (MFA) everywhere
- Use long, unique passwords
- Keep devices updated

WHY IT MATTERS

MFA blocks nearly all automated account-takeover attacks (CISA).

02

Verify Before You Trust

WHAT TO DO

- Never share codes or PINs
- Call the number on your card
- Avoid unexpected links
- Be skeptical of unexpected emails

WHY IT MATTERS

A quick pause to verify defeats most AI-driven scams (FBI).

Protect Yourself & Your Accounts

A few simple habits stop most of the fraud and cyber attacks before they start.

03

Monitor & Report Fast

WHAT TO DO

- Set transaction alerts
- Review statements and credit reports
- Report fraud fast
- Recognize and report suspicious communications

WHY IT MATTERS

Early detection sharply limits fraud loss (FBI IC3).

04

Guard Your Identity

WHAT TO DO

- Freeze your credit at all three bureaus
- Watch your credit report for accounts you didn't open
- Limit sharing your SSN and personal details

WHY IT MATTERS

A credit freeze stops criminals from opening new accounts with a stolen or synthetic identity (CFPB).