Actionable Things You & Your Employees Can Do to Prevent Future Fraud Exposures

June 20th

Presented by

Ann Davidson and Brandon Bottomley

Allied Solutions

Agenda

1. Assessing the likelihood of an attack.
2. Reviewing modern fraud landscape & threats.
3. Identifying ways to manage these **imminent** attacks against your credit union and members.

Ann Davidson

Vice President
Risk Consulting

Brandon Bottomley

Regional Vice President
Bond Specialist

Allied Solutions

Reputation Risk

This affects a financial institution's ability to meet its business objectives and preserve its image and reputation.

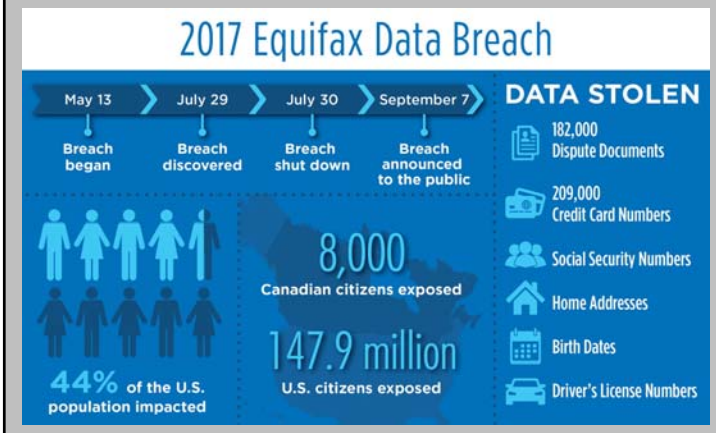
Top Fraud Risks

- Non-EMV cards & ATMs
- ATM jackpotting
- Synthetic ID theft
- Phishing attacks
- Authentication
- Data breaches
- Cyber break-ins
- Card, ACH, A2A, P2P, mobile, online
- Loans – consumer, credit card, unsecured (charge-offs)
- Check fraud – consumer & corporate
- Remote deposit capture
- ADA website compliance
- Employee dishonesty

How the Bad Guys are Breaking In

- Card fraud
- Phishing, email, text messaging or phone calls
- Data breaches
- System intrusions (includes third-parties)
- Identity theft – real or synthetic
- Authentication
- Social media / network
- New account fraud
- Account takeover fraud
- Mobile devices
- Loan fraud and collections

Fraud Landscape



Wire Fraud Mitigation

Person calls up the call center and request an outgoing wire and passes all of the authentication measures

Mitigation: Contact the member using multiple layers of risk mitigation would have mitigated the exposure

Paper Check Fraud Mitigation

Bad guy creates counterfeit CU official checks and the checks clear the risk mitigation measures

Mitigation: Positive pay/payee positive pay would have prevented the exposure

ACH Fraud Mitigation

Bad guy obtains routing and account number, breaks into the credit union, and sends an ACH credit to the RDFI and then hires money mules to withdraw the funds

Mitigation: Performing multiple layers of authentication by the originating depository financial institution (ODFI) prior to the ACH credit going out the door may have prevented the exposure

Payment Card Fraud Mitigation

Bad guy obtains card information from a data breach and creates either a “card present” or “card not present” fraud

Mitigation: Multiple layers of card security may have reduced the fraud exposure

The Many Arms of Card Fraud

ID Theft Today

Synthetic ID Theft:

- Fraudster combines fabricated info & stolen consumer info (i.e. names, birthdays, Social Security numbers, addresses)
- Individual ***does not exist***

Stolen ID Theft:

- Fraudster steals a consumer's info & takes over their real identity
- Individual ***does exist***

Synthetic ID Theft & Fraud

- Synthetic IDs are created with a real SSN
- SSN likely belongs to a person without a credit history – i.e. a minor
- Paired with fake address - even fake utility bills
- Credit history is built with the Synthetic ID
- Credit cards are taken out and used for numerous small purchases
- Synthetic Identity fraud is hitting the financial industry very hard

Risk Prevention Practices to Share with Members

- Sign up for free credit monitoring services
- Place a *freeze* on all three credit bureau accounts to prevent fraudsters from opening new accounts
- Sign up for an Identify Theft program to help in the event you are a victim of ID theft

Preventing Synthetic ID Fraud

1. Integrated suite of real-time defenses for verifying the identity of a new customer at the time of the loan/account opening
2. Multiple layers of authentication – i.e. biometrics, password, challenge questions
3. Consumer education on how to protect their personal identifiable information (PII).

Evolve Your Fraud Strategies

- Continue to adopt proven prevention methods and security tools
- Focus on faster, more effective detection of threats through a blend of people, processes, and technology
- Collect, analyze and share incident data to create a rich data source that can drive security program effectiveness
- Continue to monitor the market place to prevent becoming a victim – education is key!

Keys to Managing Fraud

- Build well-developed, fully-integrated risk strategies
- Balance consumer service with risk appetite
- Evaluate threat landscape to prioritize treatment strategy
- Don’t buy into one-size-fits-all security approach
- Commit to making tough choices
- Adopt a forward-looking strategy

Keys to Managing Fraud

- Educate members & staff frequently
- Adopt enterprise-wide risk management strategies
- Monitor all accounts across all types of activity
- Act fast on suspected attack
- Adopt multiple authentication layers
- Invest in new technologies
- Work together with risk-conscious vendors
- Keep guard up & stay tuned in

Connect with the Presenters

Ann Davidson:

ann.davidson@alliedsolutions.net

Brandon Bottomley:

brandon.bottomley@alliedsolutions.net

Allied Solutions

Additional Resources

Follow us on LinkedIn (Allied Solutions LLC) & Twitter (@alliedsolutions)

Sign-up for our *Fraud & Security Risk Alerts*: www.alliedsolutions.net/resources/Fraud-and-Security-Risk-Alert

Subscribe to our *Allied Insights* blog & newsletter: www.alliedsolutions.net/resources/allied-insights

Allied Solutions