FI Examples

1. An employee had an unencrypted laptop stolen from her automobile. BBR Services quickly connected the company with forensics to assist with assessing the information on the laptop. Once that analysis was complete, the organization learned that the laptop had contained protected information on approximately 6,000 individuals. BBR Services continued to assist by coordinating notification and call center services, as well as credit monitoring, for the affected individuals since the laptop contained their social security numbers.
2. Malware discovered on the majority of insured's computers. HR director's account was accessed and money was electronically transferred from a bank account. All 140,000 members were notified and offered credit monitoring.
3. Vendor of insured exposed mortgage holders' PII to another bank. Data included name, address, loan #, loan balance and SSN's of mortgage holders in 50 states. 67,000 notified and offered credit monitoring.
4. Insured web server was breached. Investigation was done and web server was shut down. Forensics was able to determine that a 2nd breach had occurred. Information that was breached included 5,000- 6,000 people's SSNs, driver licenses numbers, and addresses. Head of Security at the insured believes that the hackers were able to decrypt the SSNs as they were encrypted at the time of the breach.
5. Insured discovered two backup tapes missing. Forensics evaluation uncovered the tapes contained PII for 84,000 individuals.
6. Insured discovered a backup hard drive missing. Over 2,000 notifications and credit monitoring required in five different states.
7. Employee resigned and insured discovered that they had emailed themselves a spreadsheet with confidential member account numbers, names, and an indication of account size. Forensics revealed data breach affecting 9000 individuals. Notified and provided credit monitoring to all.
8. Sophisticated malware attack, where hackers were in the insured's system for at least six months. Fake accounts set up and it appears money was withdrawn from the bank from those fake accounts. Forensic investigation extremely expensive due to type of malware. Notified and provided credit monitoring to about 30,000 individuals whose Credit card numbers, SS#'s and driver's license numbers may have been exposed.
9. An employee of the insured inadvertently sent an email to a third party outside the company which contained credit union member names, account numbers and social security numbers. 621 members were affected, 379 included SSNs and 242 included just names and account numbers.
10. The Insured was notified by a third party, who insured purchased mortgages for the insured until 2013, that the mortgage service platform provided by Fiserv had never turned off a systems parameter on an interface file that would have prevented the third party from having continued access to the insured's mortgage holder personally

identifiable information. Third party has been able to inappropriately have continued access to approximately 41,600 mortgage holders' information since 2013. The data included name, address, loan #, loan balance and SSNs of mortgage holders in 50 states.

11. Insured's systems were potentially compromised due to a spear-phishing scheme that resulted in a fraudulent wire transfer and potential exfiltration of emails with customer PII. Forensics and privacy counsel concluded (after an extensive manual review of data), that the insured was legally obligated to notify 3,300 individuals.