Industry Blogs

Back to Blogs

Top 5 Tips for Emerging Payments: Fighting Fraud and Financial Crimes

February 19, 2014 Credit | Debit | Prepaid | Emerging_Technologies | Banking_Channels

Kirsten Trusko
The Network Branded Prepaid Card Association

*F*inancial systems and products are increasingly under attack, whether by organized crime, lone hactivists, or state actors. Attackers look for what they perceive as the weakest link or highest value target, to steal from or embarrass – companies, products, and industries. Often the perceived weakest link is the youngest product or company. Prepaid has lived and IS living this. Perhaps there are learnings from prepaid that are useful for other emerging financial products and for those entering prepaid.

Part of the challenge is optics. Prepaid's actual fraud losses are 16% lower than debit (source: Federal Reserve 2013 Payments Study). However, as a newer product, still little understood by government, advocates, and media – the perception has been that fraud numbers for prepaid are high.

Prepaid has made some real progress in perception over the last year. A year ago, cyber criminal forums were listing and selling data stolen from U.S. prepaid companies by brand, and teaching how to hack systems of prepaid companies Now these criminal forums increasingly list U.S. prepaid companies as having "tightened up too much" and instruct criminals to instead target foreign banks and processors.

Similarly, law enforcement's perception of prepaid has started to shift. At an NBPCA December event in New York, speakers from the FBI, U.S. Secret Service, and a prominent District Attorney's office, shared that while in the past they'd viewed prepaid as a facilitator of financial crimes, now prepaid companies are increasingly a key partner in the prevention and prosecution of crimes.

Perhaps what prepaid, as a young financial industry is doing - to correct the damaging misperception, and foil criminals - can be an example of what to do, and not to do – for other emerging financial products.

Here are the "Top 5 Tips for Fighting Financial Crimes" – across product evolution stages - in emerging financial products:

1. In initial development, get buy-in, from senior management and investors, of the importance of proactive investment in the prevention of crimes. Acknowledge that financial crimes touch brand and bottom line.

It's critical to involve senior management and investors, and together work proactively and aggressively to prevent and fight financial crimes within your organization. Preventing criminal abuse of your products isn't just a "fraud prevention" topic; it's a "brand and bottom line" topic. The media is full of examples of how financial crimes and hacking have affected brand and revenues, and its driven ill-informed rule making that affects the entire industry.

Search Perspectives
Search by Topic
Sort by Author
View All

Make prevention part of your corporate culture. Share updates and success with your teams as you would other corporate successes. Leverage your fraud prevention work as proactive and positive – as a brand and product differentiator

2. In start-up, build fraud monitoring and prevention into product development.

As you build out all aspects of your offering and infrastructure - just as you plan for product, sales, technology, service, and administration - build fighting financial crimes into the front end of any new or enhanced product. Make fraud a key part of your "people, process and technology" build at the outset, to reduce the chance your company will be a target for fraudsters, and to be ready when you're hit. Though some fraud is inevitable, through prediction and prevention, it can be minimized.

3. In ongoing operations, be nimble and quick. Be able to identify and act immediately when suspicious activity is identified. Evolve as criminals evolve.

No time can be wasted. Criminals find a weak link, share this intelligence with their networks on criminal forums, and attack hard and fast. Be prepared. Have red flags set and make plans to immediately mobilize, fix any existing weakness, and stop the targeting of your company. Have a full operational and communication plan to stop the attack, minimize its impact, and communicate with partners and customers, as appropriate. Document what you learned and feed it in as part of your continuous improvement feedback loop.

Select the best solutions/platforms for your product (versus just re-purposing existing tools). Require that fraud processes and systems evolve as your products, partners, and the criminals evolve.

4. Learn and share across industry with peers, partners, and competitors. Criminals attack the weakest link. Make your industry a hard target.

Participate in platforms and networks that enable you to actively listen and learn from your peers, partners, competitors, and law enforcement. Criminals find the weaknesses in a product set, attack one company, and then test to see if the weakness exists in other firms. Criminals quickly sell what they learn in cyber criminal forums, and suddenly the same attack is hitting entire sectors of an industry.

Find an industry group with proper sharing protocols and platforms, and share time critical information to foil fraudsters. Seek to interact -not just with your own industry - but also with those tangential who may have helpful information or who may share attackers. Learn the latest development in systems, vendors, and processes - good and bad.

Fuel the creation of industry leading practices to help set the bar. Promote, follow, and exceed these practices yourself. Strong industry level leading practices can help make your industry a hard target to hit.

5. Engage in proactive collaboration with industry to law enforcement. Fight "Organized Crime" by organizing the good guys.

Join groups to help aggregate and distill the deluge of information available across federal and state law enforcement groups. Few, if any, companies have sufficient staffing to directly engage one-to-one with the estimated 4,000+ law enforcement agencies and offices, to provide the level of responsiveness, and engagement, needed to be effective, and to build and keep these critical relationships.

Find industry groups to collectively share the critical real time information that can be directly helpful to your teams to predict, prevent, and prosecute fraudulent and criminal use of your products. A few of these groups for prepaid include: NBPCA's Financial Crimes Task Force (FCTF), NBPCA's Law Enforcement Alliance for Prepaid (LEAP), The National Cyber-Forensics & Training Alliance (NCFTA, U.S. and international), and The International Association of Financial Crimes Investigators (IAFCI, national and regional),

Because criminals are product agnostic and will jump from product to product, it's essential to gain access to information of attacks in other financial products, monitor cyber criminal forums, watch networks for botnets and malware – all to predict and prevent what could come to you. Versus traditional single account approaches, today's financial crimes are increasingly, mass system attacks – artfully coordinated to take down whole websites, jam phone lines, and infiltrate your technology and processing

capabilities at their core.

Conclusion

It's been said, "the only certainties are death and taxes". Now, add "financial crimes". The criminals are getting increasingly well organized, artfully sophisticated, incredibly orchestrated, and borderless. They organize as highly collaborative, layered, networks, developing and using the most sophisticated technology and communications available.

This is a call to action for industry – to communicate and collaborate across our financial services with colleagues AND with law enforcement, to organize proactively against Organized Crime – and make our industry a hard target. It took prepaid a few years to learn what's shared in this article, and we hope what we've learned can help other emerging financial services industries to accelerate through some of the harder steps of industry evolution.

For more information on the two NBPCA groups focused on fraud and financial crimes prevention (the Prepaid Financial Crimes Task Force and the Law Enforcement Alliance for Prepaid), please contact **preventfraud@nbpca.org** and visit **www.NBPCA.org**.

Quick Links

Advertise With Us
Recommend RSS Feed
Join Buyers Guide
Host a Strategy Session
List a Calendar Event
Give Us Feedback
Contact Mercator Advisory Group

Enter your email address GO