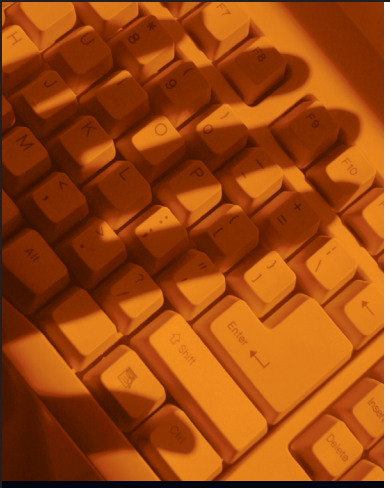

SAFETECH℠
Fraud and Security Solutions

Combat Fraud and Protect Your Bottom Line

Fraud in the insurance industry is nothing new; however, the growth of both telephone and Web-based sales channels provides fraudsters with greater opportunity to take advantage of insurance companies. The increasing threat of fraud has pushed insurance providers to evaluate multiple means to combat the threat and most insurance companies evaluate policy applicants based on a variety of factors related to the type of policy application submitted. Auto insurance policy evaluations focus almost entirely on past driving history, whereas life insurance focuses on prior medical history, age, vices and historical trend analysis. The answer to this threat – utilize a combination of best practices and proven fraud prevention tools. They can be specifically designed to detect/prevent fraud personas from replicating their scams – effectively reducing both the liability and financial impact tied to policy claims, application processing and formal fraud prevention.

THE TRADITIONAL APPROACH TO FRAUD

Insurance providers have traditionally approached fraud with a reactive strategy based on forensic investigations after a claim has been submitted. Proactive fraud prevention measures are generally limited and are restricted to availability of data for reference. For example, auto insurance policies are quoted and evaluated based on the motor vehicle record of the applicant (past negative activity including accidents); however, this information provides very little detail that can be used for fraud assessment. Use of ACH account validation and reference to a company-specific negative file (known fraudsters) is also a common method employed as part of a cursory check regarding the validity of the policy applicant. Lack of formal, real-time fraud prevention measures can be problematic in states where personal injury protection laws (PIP) require expedient payouts on policy claims. It is not uncommon for insurance carriers to forgo writing policies in PIP states due to the high degree of fraudulent activity that manifests in these areas. Fraudsters are smart, talented and, more importantly, patient. Professional fraudsters understand each state's rules and regulations that pertain to policy issuance, and they work hard to take advantage when the opportunity presents itself.

Other insurance policy types rely on third-party databases to assist with the assessment of any prior negative activity tied to an applicant. One example is the use of the industry-standard Comprehensive Loss Underwriting Exchange (CLUE) database utilized by most insurance providers in the United States. This system provides details on the prior claims activity tied to an applicant's insurance history. Consumers seeking homeowner's or renter's insurance may be evaluated based on prior claim submissions, location of the property and/or suggested property contents to be insured.The problem with these systems is that they are heavily geared toward evaluation of an individual consumer's past record (medical history, history of claims, etc.) with the goal of helping the insurance carrier

CHASE™ Paymentech

SAFETECH℠
Fraud and Security Solutions

to decide whether the applicant fits a desired profile for policy issuance and bind. They do not determine if consumers are who they say they are. A stolen identity with no prior record of negative activity may seem perfectly legitimate on the surface; however, the use of advanced fraud detection tools can track patterns of use, morphing of data and geographic variables tied to the device or persona used to apply for the policy. This allows much greater visibility into the fraud landscape.

Ultimately, insurance companies are exposed to many kinds of fraudulent activity based on the various policy types provided by the company. Professional and amateur fraudsters commonly take advantage of insurance providers with a variety of scams, from false claims payouts to vehicle registration scams (using falsified insurance). Auto insurance fraud, in numerous iterations, is one of the most challenging obstacles faced by insurance companies today. The following section outlines several common fraud schemes operating against U.S.-based insurance carriers today.

Types of Fraud Tied to Card-Not-Present (CNP) Insurance Applications

Malware Attacks (Web applications) – Malicious software (trojans, botnets, worms) that has the purpose of stealing identities or data from unsuspecting businesses or consumers. Malware can be used to collect financial data, contact data or passwords to commit fraudulent purchases or set up fraudulent lines of credit. Malware attacks often go undetected as part of online commerce due to the sophistication of the software, as well as considerable emphasis placed by the fraudsters on anonymizing their identify. Botnets may include several hundred (or thousands) of "slave" computers that are utilized to initiate a string of fraudulent policy applications using stolen consumer data. Detecting the source of the fraud is a difficult challenge faced by insurance companies today.

Pharming (Web applications) – Systematic redirection of a consumer's Web browser to a fraudulent Web site. That Web site may have the look and feel of the actual merchant Web site, but is designed to capture the consumer's information for malicious use.

Phishing (Web applications) – Fraudulent e-mails sent to consumers disguised as credential verification requests from the insurer. This is a very common method for identity takeovers. Similar scams involve text messaging (SMSishing) and voice mail (vishing).

Amateur Fraud (all CNP sales channels) – Unsophisticated fraudsters use stolen consumer information to apply for falsified insurance policies. These amateur fraudsters tend to use similar common data elements (such as billing address, phone number and customer name). Amateur fraud includes the concept of "friendly fraud" as well, where a consumer may use their own name and address details to apply for a policy with the intent to defraud the carrier via false claims.

Fraudulent Claims (all policy types) – False claims represent one of the most significant forms of lost revenue for insurance companies today. They come in many forms, the most common element being a fraudster applying for a false policy using legitimate or stolen consumer data. Although this process is pervasive across many types of insurance, it is particularly challenging in the auto insurance space. PIP laws, which require expedient payouts on claims, dramatically reduce the amount of time a carrier can devote to evaluating fraud from a claims submission. PIP laws apply in states like New York and Florida, where the occurrence of fraudulent activity has traditionally been extremely high.

Quote Scams (all policy types) – It's not uncommon for insurance companies to see quote-to-policy conversion rates that are 10:1

Auto insurance fraud, in numerous iterations, is one of the most challenging obstacles faced by insurance companies today.

CHASE™ Paymentech

SAFETECH℠
Fraud and Security Solutions

(or higher). There is a significant cost associated with collecting consumer information, pulling motor vehicle records (or reviewing past medical history) and quoting a consumer a policy rate. Some legitimate consumers may seek multiple quotes from a given insurance carrier, trying to "game" the system for the best possible rate. Consumers may change their billing address (using a relative or friend's address, for example) to try to obtain a better quote for insurance. This represents a type of fraud that does not necessarily translate to a claim; however, the cost tied to quoting (and re-quoting) these individuals can be extremely high, as each motor vehicle record check (for auto insurance) can cost anywhere from $2 - $20 per record request. Plus, fraudsters are certainly using stolen identities with the intent to obtain fraudulent policies. They may systematically approach various insurance companies, applying for multiple policies using the same stolen consumer profile.

Insurance Card Scams (auto insurance) – This is a common fraudulent practice in which a consumer may use a stolen identity to obtain an insurance card to enable their vehicle registration process. In many states, proof of liability insurance is a fundamental requirement to obtain vehicle registration from the Department of Motor Vehicles (DMV). Consumers who have a history of accidents or prior claims; legal action; or other negative event may seek any way possible to obtain proof of insurance so that they can register their vehicle. The consumer may not particularly care about the validity of the policy as long as they can get their vehicle registered.

Refund Fraud (all policy types) – Increasingly, fraudsters may use a stolen identity to create an insurance policy, then attempt to overpay the policy premium by a certain amount in an effort to obtain a refund check from the carrier. This is common in the auto insurance process, where the scrutiny around claims fraud far outweighs what may be perceived to be a simple overpayment by a policy holder. This practice clearly leads to both the loss of the refund amount as well as the costs tied to chargebacks or ACH returns.

Increasingly, fraudsters may use a stolen identity to create an insurance policy, then attempt to overpay the policy premium by a certain amount in an effort to obtain a refund check from the carrier.

Broker Scams – Insurance carriers may have a network of licensed brokers who submit policy applications on behalf of their clients. While consumers may create false policies via one of these channels, a larger challenge is the use of this channel by fraudsters who market themselves as a discount broker of insurance (typically auto insurance). Unlicensed brokers (fraudsters) may set up shop, typically in low-income communities where they will accept cash for policies created using stolen identities. The false broker leverages the online sales process of an insurance carrier due to the anonymous nature of the transaction. That broker then takes the cash from this activity and moves from community to community plying his/her trade. The damage caused in this process is multifold.

- The broker may be stealing from legitimate consumers while using the insurance carrier resources to vet a false policy application.
- A consumer may use a fraudulent broker to obtain false proof of insurance so that they can register their car. The insurance carrier is subject to both a chargeback/return for the stolen identity as well as potential reputation damage when an unlicensed broker claims association with the insurance company.
- The insurance carrier must pay any costs for DMV record research for each quote. These costs may be considerable, depending on the size of the fraudulent broker's operation.

Fraud Prevention Strategies

Set Purchase Limits – Limit the number of policies and/or the amount tied to policy creation in a 24-hour period. Fraudsters hit hard and fast, and will try to max out the stolen credit cards they have.

Monitor Bill to/Ship to Mismatches – Pay particular attention to this category. Different billing and shipping addresses are commonly associated with fraud; however, it's important to consider this to be one factor out of many. It's not uncommon for relatives or friends to pay for the insurance policy for someone else. It's also common for insurance applicants to use different addresses for billing or registration of a vehicle (for example).

SAFETECH℠
Fraud and Security Solutions

Pay Attention to the Time of Day – The adage "nothing good ever happens after midnight" applies to insurance as well. Pay particular attention to the location of the consumer (use IP mapping/proxy piercing technology) and be wary of policy applications placed late at night or early in the morning.

Ask a Secret Question – Offer a secret question used at the time of registration and specify it to prompt periodically used when users attempt to log into their account. This can help prevent account takeovers.

Manage Passwords – Force users to change their passwords periodically to fight phishing scams. This applies to insurers who allow username and password registration (payment method/user credential storage).

Account Change Notification – Merchants should take great care in notifying their users about any changes to their account (via e-mail notification).

Employ Velocity Checks – Control number of cards/ACH accounts that can be used by a registrant and the total number of policy applications created in a given day. The velocity concept applies to purchase use patterns and dollar limits as well. Very few consumers will use more than a handful of credit cards to make a purchase. Be wary of any consumer who attempts to use three or more cards to make a purchase in a short period of time.

Use Auto Accept/Reject – Utilize fraud technologies that can compare data elements in real time. For those orders where further review is required, consider using solutions that allow for secondary review rules that can call out to external phone numbers and/or address validation services.

Minimize Manual Review – Keep manual review to a minimum through the use of real-time fraud detection tools. Do not exceed 10-percent review as an average. Leverage tools that provide greater visibility into order data, purchase history and geolocation information to prevent the acceptance of fraudulent orders. If reviewers are approving over 30 percent of orders sent to the review queue, then too many good orders are being flagged for review.

Use Proxy Piercing/IP Geolocation Technology – Prevent fraud with technologies that are able to pierce proxy or other identity-obscuring attempts by the consumer. The insurer can see the geolocation of the consumer/fraudster in question by state or country relative to the information provided during the purchase.

Apply Device Fingerprinting Technology – Fingerprinting devices associated with online purchases can provide tremendous visibility/insight into fraud patterns. Multiple computers placing multiple orders are generally detectable by multi-layer device fingerprinting technology.

Implement Multi-merchant Order Linking – Software designed to look at over 200 data elements while comparing that information against other order data in real time. Fraudulent use patterns can be tied back to other orders that would otherwise go unnoticed by the human eye.

Adopt Dynamic Risk Scoring – Deploy a solution that provides a real time assessment of the validity of a purchaser that includes constant rescoring of the order information compared against any new or historic transaction information. The order billing information may be any combination of the following: name, card number, billing/shipping address, IP address, e-mail, phone number, device ID/location, velocity and purchase patterns. This type of solution allows insurance companies visibility into changing fraud trends within the game including account takeovers. What appears good one day may turn bad the next.

Maintain Positive and Negative Lists – Protect good customers from unnecessary scrutiny and place known or suspected "bad" customers on a negative list. Pay particular attention to changes in core data elements associated with "good" customers and follow up with a review.

Apply Custom Fraud Business Rules – Merchant-specific business rules created and stored in a virtual, Software-as-a-Service-based environment can be highly predictive of fraudulent patterns when used in conjunction with many of the core fraud tools described above.

Evidence suggests that a clear description of service and terms of sales can reduce consumer-based perception of fraud.

CHASE™
Paymentech

SAFETECH℠
Fraud and Security Solutions

There are no silver bullets when it comes to fraud prevention; however, the use of a proactive fraud assessment strategy that combines multiple, proven fraud-fighting technologies with adherence to best practices can offer insurance carriers a significant advantage in their fight against fraud. The goal isn't to eliminate fraud altogether; fraud is a fact of life in the insurance industry and it's here to stay. Insurance carriers can manage their level of exposure by adapting quickly to changing fraud trends through the use of enterprise-class, fraud-prevention tools specifically designed to detect global fraud patterns. The combination of cutting-edge fraud tools with over a century of experience in forensic claims investigation can serve as an effective, proactive fraud-prevention strategy for any company in the insurance space.

POLICY ACCEPTANCE BEST PRACTICES

Have a Clear, Prominent Description.

- Evidence suggests that a clear description of service and terms of sales can reduce consumer-based perception of fraud. Some chargebacks and ACH returns can be avoided through a clear description of services provided, effectively reducing the likelihood that a consumer won't remember the purchase and think the transaction is fraudulent.

Provide Consultative Customer Service.

- Refunds, whether partial or full, can go a long way in satisfying unhappy customers. Insurance carriers should have tight controls for issuing refunds. This is one of the most common ways to circumvent a chargeback or ACH return; however, it's also one of the most widely overlooked costs associated with fraud prevention. Having low chargebacks/returns (under 0.50 percent) with a high rate of refunds (1 percent or more) is a sign of a significant issue.
- Some chargebacks/returns can be avoided by working with the consumers to remind them which policy or policies were purchased, including details around coverage and payment terms. Some fraud can be avoided through customer service and education. An example of this is when a customer uses a relative's payment data to sign up for a policy.
- Do not allow customer service representatives too much latitude in identifying possible fraud. Fraudsters prey on sales channels where inconsistency and personality are a common element. Use a specific set of questions designed to verify customer information as well as formal fraud tools. Remove the human element from the equation and focus on the facts.

Use Payment Industry Fraud Prevention Tools.

- **Address Verification Service (AVS)** – you can eliminate some amateur fraudsters with simple AVS checks; however, this simple fraud mechanism should never be used as a standalone fraud measure due to the high degree of false positives that may arise. This is a credit card payment-specific response from the credit card-issuing bank, indicating a match, non-match or partial match of the first five digits and the last five digits (ZIP code) of the billing address included in the transaction.
- **Card Verification Numbers (CVN)** – Card verification numbers can be a reasonable detector of amateur fraud on global transactions. The CVN number refers to the last three digits in the signature panel of a Visa, MasterCard or Discover Card or the four digits above the card number on the front of an American Express card.
- **www.whitepages.com** – address and reverse phone number lookup
- **www.pipl.com** – address and phone number association to a name
- **www.anywho.com** – address and reverse phone number lookup
- **Google Search** – "phonebook:XXX-XXX-XXXX"

Do not give fraudsters the intelligence they need to continue stealing from your Web site.

CHASE™ Paymentech

SAFETECH℠
Fraud and Security Solutions

Insurance carriers can manage their level of exposure by adapting quickly to changing fraud trends through the use of fraud-prevention tools designed to detect global fraud patterns.

- **Google Earth** – Useful tool to verify/see the physical location associated with the shipping address provided. If it's a hotel, shopping center (PO Box), warehouse, or generally odd location further verification should be engaged before accepting the order.

Monitor Chargeback and ACH Return Analysis.

- Pay attention to the various chargeback/return codes and group by category. Not all fraud chargebacks are classified as identify theft, e.g., "services/merchandise not received." Each bank is responsible for classified chargeback/return filings from consumers. Unfortunately, many of these are misclassified and often missed by fraud departments who are reviewing transactions for fraud. It's also common for friendly fraudsters (fraudsters using their own address and payment data) to initiate a chargeback or return with a classification that is not fraud-related. This may allow the friendly fraudster to apply for a policy, obtain coverage and then claim they never signed up to begin with.

Offer Order Status Messaging.

- Accept every policy application (except those with credit card declines) and cancel those deemed to be fraudulent by sending an e-mail to the e-mail address provided by the consumer.
- Offer another way to purchase (for those that are rejected) by providing a customer service phone number where they can complete their order. Legitimate consumers who are falsely identified as fraudulent will tend to pick up the phone to complete their purchase. Fraudsters who attempt to call can typically be weeded out by asking for the billing and card verification number data used to make the purchase and validating that information against formal fraud prevention measures used internally.

CHASE™ Paymentech